Algèbre

Université du Luxembourg

Gabor Wiese
gabor.wiese@uni.lu

Version du 16 janvier 2021

Table des matières

Préface

L'objet principal du cours sera l'étude des anneaux et des extensions algébriques des corps commutatifs. En particulier, la théorie de Galois sera développée et appliquée. Elle permet entre autres de démontrer que l'équation générale de degré au moins 5 ne peut pas être résolue en radicaux et de résoudre (parfois de manière négative) plusieurs problèmes classiques (provenant des Grecs anciens) de construction à la règle et au compas comme la trisection d'un angle et la quadrature du cercle.
Le cours est basé sur des notes de cours donnés par Denis Vogel, Alexander Schmidt et B.H. Matzat. Il est assez (parfois très) proche du livre de Bosch (voir ci-dessous).

Littérature

Voici quelques références sur la théorie de Galois en français :

- Jean-Pierre Escoffier : *Théorie de Galois*
- Jean-Claude Carrega : *Théorie des corps, la règle et le compas*
- Antoine Chambert-Loir : *Algèbre corporelle*
- Yvan Gozard : *Théorie de Galois*
- Patrice Tauvel : *Corps commutatifs et théorie de Galois*
- Josette Calais : *Extension de corps, théorie de Galois*
- Evariste Galois : le texte original !

Voici quelques d'autres références :

- Siegfried Bosch : *Algebra* (en allemand), Springer-Verlag. Ce livre est très complet et bien lisible.
- Ian Stewart : *Galois Theory*. Ce livre est bien lisible. Le traitement de la théorie de Galois dans le cours sera un peu plus général puisque Stewart se restreint dans les premiers chapitres aux sous-corps des nombres complexes.
- Serge Lang : *Algebra* (en anglais), Springer-Verlag. C'est comme une encyclopédie de l'algèbre ; on y trouve beaucoup de sujets rassemblés, écrits de façon concise.

Conventions

- Nous ne devons jamais oublier qu'un groupe est un triplet $(G, \circ, e)$ où G est l'ensemble des éléments de G, $\circ$ désigne la loi de groupe (loi interne) et e est l'élément neutre. On peut évidemment choisir n'importe quel symbole. Des symboles souvent utilisés pour la loi de groupe sont $\cdot$, $+$, $\times$, $*$, $\circ$, mais on pourrait aussi choisir `BelleMultiplication`.

- Souvent on n'a pas envie d'écrire le triplet et on n'écrit que $(G, \circ)$ ou bien « G pour la loi $\circ$ ». Dans ce cas, on écrit souvent e_G ou juste e pour l'élément neutre. Normalement, une confusion est impossible car il n'y a qu'un seul élément neutre dans le groupe (comme on l'a démontré en Algèbre 1).

- Si la loi de groupe est un symbole qui rappelle la multiplication comme $\cdot$, $\times$, $*$, $\circ$, $\otimes$, on écrit souvent 1 pour l'élément neutre ; dans ce cas on note g^{-1} l'inverse d'un élément g du groupe. Par contre, si le symbole rappelle l'addition comme $+$, $\oplus$, l'élément neutre s'écrit 0 (au lieu de 1, car l'égalité $1 + 1 = 1$ serait trop bizarre) et $-g$ est l'inverse de g. La notation additive est en général réservée aux groupes commutatifs.

- Si nous écrivons « Soit G un groupe » sans spécifier ni la loi de groupe ni l'élément neutre, on utilise un symbole multiplicatif comme $\cdot$, $\times$ (selon votre et notre goût) pour la loi de groupe et 1 pour l'élément neutre.

- Dans ce cours nous supposons que tout corps est commutatif. Donc nous utilisons le mot « corps » pour signifier « corps commutatif ».

- En plus, la plupart des anneaux seront commutatifs : sauf si le contraire est mentionné explicitement, nous supposons les anneaux commutatifs.

- Dans un anneau, l'inverse pour l'addition d'un élément a est noté $-a$ et on écrira $a - b$ pour $a + (-b)$.

Rappel de structures fondamentales

Cette section contient un rappel des structures fondamentales introduites dans le cours *Structures mathématiques* du 1er semestre. Le cours magistral commencera par la prochaine section.

Groupes

Définition 0.1. *On appelle* groupe (group, Gruppe) *tout ensemble G contenant un élément $e \in G$ et muni d'une application (*loi interne, loi de groupe*)*

$$* : G \times G \to G$$

tel que

Associativité : $\forall\, g_1, g_2, g_3 \in G :\ (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$,

Élément neutre : $\forall\, g \in G : e * g = g * e = g$ *et*

Existence d'inverse : $\forall\, g \in G\ \exists\, h \in G : h * g = g * h = e$.

Un groupe consiste donc en les données : $(G, *, e)$.
Un groupe $(G, *, e)$ *est appelé* commutatif *ou* abélien *si*

Commutativité : $\forall\, g_1, g_2 \in G : g_1 * g_2 = g_2 * g_1$.

Exemple 0.2.
- $(\mathbb{Z}, +, 0)$ *est un groupe abélien.*
- *Le groupe symétrique* $(S_n, \circ, (1))$ *est un groupe non-abélien dès que* $n \geq 3$.
- *On note* $\mathrm{Mat}_n(\mathbb{R})$ *les matrices réelles d'ordre* n *(*$n \in \mathbb{N}$*). Alors,* $(\mathrm{Mat}_n(\mathbb{R}), +, \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix})$ *est un groupe abélien. On écrira aussi* 0 *pour l'élément neutre de ce groupe.*
- *On note*

$$\mathrm{GL}_n(\mathbb{R}) := \{M \in \mathrm{Mat}_n(\mathbb{R}) \mid M \text{ est inversible } \} = \{M \in \mathrm{Mat}_n(\mathbb{R}) \mid \det(M) \neq 0\},$$

appelé le groupe général linéaire. *Alors,* $(\mathrm{GL}_n(\mathbb{R}), \circ, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix})$ *est un groupe où* $\circ$ *est la multiplication des matrices (voir vos cours d'algèbre linéaire). On écrira aussi* 1 *pour l'élément neutre de ce groupe. Ce groupe n'est pas abélien dès que* $n > 1$. *Trouvez vous-même un exemple de matrices qui ne commutent pas !*

Anneaux et corps

Définition 0.3. *On appelle* anneau (Ring) *tout ensemble* A *contenant deux éléments (pas nécessairement distincts) et muni de deux applications*

$$+_A : A \times A \to A, \quad \text{et} \quad \cdot_A : A \times A \to A$$

tel que

Groupe additif : $(A, +_A, 0_A)$ *est un groupe abélien,*

Associativité : $\forall\, a, b, c \in A :\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$,

Élément neutre : $\forall\, a \in A : 1_A \cdot a = a \cdot 1_A = a$ *et*

Distributivité : *Pour tous* $a, b, c \in A$ *:*

$$a \cdot_A (b +_A c) = (a \cdot_A b) +_A (a \cdot_A c)$$

et

$$(a +_A b) \cdot_A c = (a \cdot_A c) +_A (b \cdot_A c).$$

Un anneau consiste donc en les données : $(A, +, \cdot, 0_A, 1_A)$ *(nous écrirons* $0 = 0_A$ *et* $1 = 1_A$ *dans la suite).*
Un anneau $(A, +, \cdot, 0_A, 1_A)$ *est appelé* commutatif *si*

Commutativité : $\forall\, a, b \in A :\ a \cdot b = b \cdot a$.

Dans la littérature, ce que nous appelons *anneau* est souvent appelé *anneau unitaire* pour souligner l'existence d'un élément neutre pour la multiplication. La plupart des anneaux dans ce cours seront commutatifs.

Exemple 0.4.

- $(\mathbb{Z}, +, \cdot, 0, 1)$ *est un anneau commutatif.*
- $(\mathrm{Mat}_n(\mathbb{R}), +, \circ, \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix})$ *est un anneau. Il n'est pas commutatif dès que* $n \geq 2$.

Définition 0.5. *Soit* $(A, +, \cdot, 0, 1)$ *un anneau commutatif.*

- *Soient* $u, v \in A$. *On dit que* u divise v *s'il existe* $q \in A$ *tel que* $v = q \cdot u$.
- *On appelle* unité *tout élément* $u \in A$ *tel qu'il existe un* $q \in A$ *qui satisfait* $1 = q \cdot u$.

  Une unité est donc un diviseur de 1. *On peut aussi caractériser les unités comme les éléments inversibles dans le monoïde* $(A, \cdot, 1)$.

  L'ensemble des unités de A *est noté* $A^\times$. $(A^\times, \cdot, 1)$ *est un groupe (abélien comme l'anneau est commutatif). On l'appelle le* groupe des unités de A.
- *On appelle* diviseur de zéro *tout élément* $u \in A$ *tel que* u *divise* 0 *pour* $q \neq 0$, *c'est-à-dire, tel qu'il existe* $q \in A \setminus \{0\}$ *avec* $0 = q \cdot u$.
- *L'anneau* A *est dit* intègre *si le seul diviseur de zéro est* 0. *C'est-à-dire que pour tout* $u, v \in A \setminus \{0\}$ *on a* $u \cdot v \neq 0$.

Définition 0.6. *Soit* $(A, +, \cdot, 0, 1)$ *un anneau (commutatif). On l'appelle* corps (commutatif) *si*

- *tout* $0 \neq a \in A$ *est une unité pour la multiplication (c'est-à-dire,* $A^\times = A \setminus \{0\}$*) et*
- $0 \neq 1$.

Remarque 0.7. *Traductions :*

- *Anglais :* field *veut dire « corps commutatif ».*
- *Anglais :* skew field *veut dire « corps non-commutatif ».*
- *Allemand :* Körper *veut dire « corps commutatif ».*
- *Allemand :* Schiefkörper *veut dire « corps non-commutatif ».*
- *Néerlandais :* lichaam *veut dire « corps commutatif ».*

- *Flamand :* veld *veut dire « corps commutatif ».*

Donc, dans les langues différentes du français, il semble que tout corps est automatiquement commutatif.
Dans ce cours nous supposons aussi que tout corps est commutatif. *Donc nous utilisons le mot « corps » pour signifier « corps commutatif ».*

Exemple 0.8.
- $(\mathbb{Q}, +, \cdot, 0, 1)$ *est un corps.*
- $(\mathbb{R}, +, \cdot, 0, 1)$ *est un corps.*
- $(\mathbb{Z}, +, \cdot, 0, 1)$ *n'est pas un corps.*
- *Soit p un nombre premier. $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot, \overline{0}, \overline{1})$ est un corps fini à p éléments.*

Homomorphismes de groupes et sous-groupes

Les homomorphismes sont des applications qui préservent toutes les structures. Ainsi, les homomorphismes de groupes préservent la loi de groupe et l'élément neutre.

Définition 0.9. *Soient $(G, \star, e)$ et $(H, \circ, \epsilon)$ deux groupes. On appelle* (homo)morphisme de groupes *toute application*

$$\varphi : G \to H$$

telle que pour tout $g_1, g_2 \in G$ on a

$$\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2).$$

On utilise la notation $\mathrm{Hom}(G, H)$ pour l'ensemble des homomorphismes de groupes de G dans H.

Lemme 0.10. *Soit $\varphi : G \to H$ un homomorphisme de groupes. Alors $\varphi(e) = \epsilon$.*

Démonstration. Comme $e \star e = e$, nous avons $\varphi(e) = \varphi(e \star e) = \varphi(e) \circ \varphi(e)$. Cela implique

$$\epsilon = \varphi(e) \circ \varphi(e)^{-1} = (\varphi(e) \circ \varphi(e)) \circ \varphi(e)^{-1} = \varphi(e) \circ (\varphi(e) \circ \varphi(e)^{-1}) = \varphi(e) \circ \epsilon = \varphi(e).$$

□

Exemple 0.11.
- $\varphi : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto 2n$, *définit un homomorphisme de groupes de $(\mathbb{Z}, +, 0)$ dans lui-même.*
- *Le déterminant* $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ *définit un homomorphisme de groupes de* $\mathrm{GL}_n(\mathbb{R})$ *dans le groupe des unités de $\mathbb{R}$ (qui est égal à $\mathbb{R} \setminus \{0\}$ car $\mathbb{R}$ est un corps).*

  Si la loi de groupe ainsi que l'élément neutre sont clairs, on les supprime (comme dans cet exemple).
- *Pour des propriétés importantes, voir le cours* Structures mathématiques.

Définition 0.12. *Soient $(G, \cdot, e)$ un groupe. On appelle* sous-groupe de G *tout sous-ensemble $H \subseteq G$ tel que*

- $e \in H$,
- *pour tous* $a, b \in H$ *on a* $a \cdot b \in H$ *(donc,* $\cdot$ *se restreint en une application* $H \times H \to H$*), et*
- *pour tout* $a \in H$*, l'inverse* $a^{-1} \in H$.

Notation : $H \leq G$.

Définition 0.13. *Soient* $(G, \star, e)$ *et* $(H, \circ, \epsilon)$ *des groupes et* $\varphi : G \to H$ *un homomorphisme de groupes. Le* noyau de φ *est défini comme*

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = \epsilon\}.$$

Exemple 0.14. *Soit* $n \in \mathbb{N}_{\geq 1}$ *et* $(S_n, \circ, (1))$ *le groupe symétrique. On rappelle qu'on définit l'application* signe (ou signature) *par*

$$\mathrm{sgn} : S_n \to \{+1, -1\}, \quad \pi \mapsto \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}.$$

C'est un homomorphisme de groupes. Son noyau est noté A_n *et appelé le* groupe alterné.
Le signe de toute transposition $(i \quad j)$ *(avec* $i \neq j$*) est* -1.

Lemme 0.15. *Le noyau d'un homomorphisme de groupes* $\varphi : G \to H$ *est un sous-groupe.*

Démonstration. Comme $\varphi(e) = \epsilon$, on a $e \in \ker(\varphi)$. Soit $g_1, g_2 \in \ker(\varphi)$, donc $\varphi(g_1) = \varphi(g_2) = \epsilon$, d'où $\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2) = \epsilon \circ \epsilon = \epsilon$ et $g_1 \star g_2 \in \ker(\varphi)$. Finalement, si $g \in \ker(\varphi)$ on a $\epsilon = \varphi(e) = \varphi(g \star g^{-1}) = \varphi(g) \circ \varphi(g^{-1}) = \epsilon \circ \varphi(g^{-1}) = \varphi(g^{-1})$, d'ou $g^{-1} \in \ker(\varphi)$. □

La proposition suivante est très utile.

Proposition 0.16. *Nous avons l'équivalence :*

$$\varphi \text{ est injectif } \Leftrightarrow \ker(\varphi) = \{e_1\}.$$

Une telle proposition est aussi valable pour les applications linéaires entre espaces vectoriels (voir cours d'algèbre linéaire).

1 Homomorphismes et isomorphismes de groupes

Objectifs :

- Apprendre et maîtriser la notion de sous-groupe distingué ;
- connaître la définition de quotients d'un groupe par un sous-groupe distingué ;
- connaître pourquoi la normalité est nécessaire ;
- savoir calculer dans les quotients ;
- connaître et savoir appliquer les théorèmes d'isomorphisme ;
- savoir démontrer des propriétés simples.

Sous-groupes distingués

Si rien d'autre n'est écrit, la loi de groupe pour tout groupe G est écrit comme une multiplication et l'élément neutre est noté 1 ou e. On commence par rappeler la définition des classes à gauche suivant en sous-groupe.

Définition-Lemme 1.1 (voir Structures mathématiques)**.** *Soit G un groupe et $H \leq G$ un sous-groupe. La relation définie par*

$$g_1 \sim_H g_2 \quad :\Leftrightarrow \quad g_1^{-1} \cdot g_2 \in H$$

est une relation d'équivalence.
Les classes d'équivalence sont de la forme

$$gH = \{g \cdot h \mid h \in H\}$$

et elles s'appellent classes à gauche de G suivant H. *On a $1H = 1 \cdot H = H$. L'ensemble de ces classes est noté G/H.*
Donc, on a

- $G = \bigsqcup_{gH \in G/H} gH$,
- $g_1H \cap g_2H = \begin{cases} \emptyset & \text{si } g_1^{-1}g_2 \notin H, \\ g_1H = g_2H & \text{si } g_1^{-1}g_2 \in H. \end{cases}$

Un élément $g_2 \in g_1H$ est appelé un représentant *de la classe g_1H. On a alors $g_1H = g_2H$.*

Démonstration. La vérification que c'est une relation d'équivalence est un exercice. Le reste est une conséquence valable pour toutes les relations d'équivalence. □

Similairement, on définit les *classes à droite suivant H* comme les ensembles

$$Hg = \{hg \mid h \in H\}$$

et l'ensemble des classes à droite est noté $H\backslash G$.

Définition 1.2. *On appelle* norma *ou* distingué *tout sous-groupe $H \leq G$ (notation : $H \trianglelefteq G$; anglais : normal subgroup, allemand : Normalteiler) tel que*

$$\forall\, h \in H,\, \forall\, g \in G :\ g^{-1}hg \in H.$$

Exemple 1.3. *Si G est abélien, tout sous-groupe $H \leq G$ est distingué car $g^{-1}hg = hg^{-1}g = h \cdot 1 = h \in H$ pour tout $g \in G$ et tout $h \in H$. En particulier, le sous-groupe $n\mathbb{Z}$ de $(\mathbb{Z}, +, 0)$ (pour $n \in \mathbb{N}$) est distingué.*

Proposition 1.4. *Soit $\varphi : G \to L$ un homomorphisme de groupes.*

(a) $\ker(\varphi) \trianglelefteq G$ *est un sous-groupe distingué.*

(b) Si $H \trianglelefteq L$ est un sous-groupe distingué, alors l'image réciproque $\varphi^{-1}(H) \trianglelefteq G$ est un sous-groupe normal.

(c) Si φ est surjectif et $H \trianglelefteq G$ est un sous-groupe distingué, alors l'image $\varphi(H) \trianglelefteq L$ est un sous-groupe distingué.

Démonstration. (a) suit de (b) pour $H = \{1\} \trianglelefteq L$.
(b) Soit $x \in \varphi^{-1}(H)$, donc $\varphi(x) \in H$. Soit $g \in G$. Alors

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in H,$$

donc $gxg^{-1} \in \varphi^{-1}(H)$, montrant que $\varphi^{-1}(H)$ est un sous-groupe distingué de G.
(c) Soit $\varphi(h) \in \varphi(H)$. Soit $\ell \in L$. Par surjectivité de φ, nous avons $\ell = \varphi(g)$ pour un $g \in G$. Donc

$$\ell^{-1}\varphi(h)\ell = \varphi(g)^{-1}\varphi(h)\varphi(g) = \varphi(g^{-1}hg) \in \varphi(H)$$

car $g^{-1}hg \in H$, montrant que $\varphi(H)$ est un sous-groupe distingué de L. □

Exemple 1.5. *Soit $n \in \mathbb{N}_{\geq 2}$. Alors, le groupe alterné A_n est un sous-groupe distingué du groupe symétrique S_n car c'est le noyau de* sgn.

Lemme 1.6. *Soit G un groupe et $H \subseteq G$ un sous-groupe. Alors les assertions suivantes sont équivalentes :*

(i) $H \subseteq G$ est un sous-groupe distingué.

(ii) Pour tout $g \in G$ on a $gH = Hg$.

(iii) Pour tout $x, x', y, y' \in G$ on a : $xH = x'H \ \wedge\ yH = y'H \Rightarrow (xy)H = (x'y')H$.

Démonstration. « (i) ⇒ (ii) » : Soit $g \in G$. Par (i) nous avons $g^{-1}Hg \subseteq H$, donc $Hg \subseteq gH$. En appliquant (i) aussi avec g^{-1} (au lieu de g), nous obtenons $gH \subseteq Hg$, donc l'égalité $gH = Hg$.
« (ii) ⇒ (iii) » : Soient $x, x', y, y' \in G$. On pose $g = y$, $h = x^{-1}x' \in H$ et $h' = y^{-1}y' \in H$. Alors par (ii) nous avons $g^{-1}hg \in H$, donc $g^{-1}hgh' = y^{-1}x^{-1}x'yy^{-1}y' = y^{-1}x^{-1}x'y' \in H$, donc $x'y' \in (xy)H$ et alors $x'y'H \subseteq (xy)H$. En échangeant les rôles ($x \leftrightarrow x'$, $y \leftrightarrow y'$), on obtient l'inclusion dans l'autre sense et alors $(xy)H = (x'y')H$.
« (iii) ⇒ (i) » : Soient $g \in G$ et $h \in H$. On pose $y = y' = g$, $x = 1$ et $x' = h$. Cela donne par (iii) : $g^{-1}hg = y^{-1}x^{-1}x'y' \in H$. □

Quotients

La normalité d'un sous-groupe $H \subseteq G$ nous permet de définir une loi de groupe sur G/H.

Proposition 1.7. *Soit $(G, \cdot, 1)$ un groupe et $H \trianglelefteq G$ un sous-groupe normal.*

(a) L'application

$$\star : G/H \times G/H \to G/H, \quad (g_1H, g_2H) \mapsto g_1H \star g_2H := (g_1g_2)H$$

est bien définie, c'est-à-dire, ne dépend pas des choix des représentants des classes.

(b) $(G/H, \star, H)$ est un groupe, appelé quotient de G par H (en allemand on dit soit Quotient soit Faktorgruppe).

(c) L'application

$$\pi : G \to G/H, \quad g \mapsto gH$$

est un homomorphisme de groupes surjectif, appelé projection naturelle. *On a* $\ker(\pi) = H$.

Démonstration. (a) En effet, le lemme 1.6 montre que la définition ne dépend pas du choix des représentants.
(b)

Associativité $(g_1H \star g_2H) \star g_3H = (g_1g_2)H \star g_3H = ((g_1g_2)g_3)H = (g_1(g_2g_3))H = g_1H \star (g_2g_3)H = g_1H \star (g_2H \star g_3H)$ pour tout $g_1H, g_2H, g_3H \in G/H$.

Existence du neutre $gH \star H = (g1)H = gH$ pour tout $gH \in G/H$.

Existence d'inverse $gH \star g^{-1}H = (gg^{-1})H = H$ pour tout $gH \in G/H$.

(c)

Surjectivité Clair.

Homomorphisme $\pi(gh) = (gh)H = gH \star hH = \pi(g) \star \pi(h)$ pour tout $g, h \in G$.

Noyau $\pi(g) = gH = H$ si et seulement si $g \in H$.

□

Exemple 1.8. $(\mathbb{Z}/n\mathbb{Z}, +, \overline{0})$ *est le quotient de* $(\mathbb{Z}, +, 0)$ *par le sous-groupe distingué* $(n\mathbb{Z}, +, 0)$.

Dans les exercices nous voyons un point de vue alternatif sur les quotients. On pourrait le regarder comme plus élégant et plus facile (selon les goûts).

Proposition 1.9. *Soit G un groupe.*

(a) Soient $E, F \subseteq G$ des sous-ensemble. Nous définissons

$$E \cdot F = \{e \cdot f \mid e \in E, f \in F\}.$$

Alors on a l'associativité :

$$E_1 \cdot (E_2 \cdot E_3) = (E_1 \cdot E_2) \cdot E_3$$

pour tous sous-ensembles $E_1, E_2, E_3 \subseteq G$.

(b) Soit $H \subseteq G$ un sous-groupe. Alors on a : $H \cdot H = H$.

(c) Soient $H \subseteq G$ et $g \in G$. Nous abusons (légèrement) la notation pour écrire $g \cdot H$ pour $\{g\} \cdot H$, la classe à gauche suivant H représentée par g. Supposons que $H \trianglelefteq G$ soit normal.

Alors pour tout $g_1, g_2, g_3 \in G$ on a :

(1) $(g_1 \cdot H) \cdot (g_2 \cdot H) = (g_1 \cdot g_2) \cdot H$,

(2) $(g_1 \cdot H) \cdot H = H \cdot (g_1 \cdot H) = g_1 \cdot H$,

(3) $\big((g_1 \cdot H) \cdot (g_2 \cdot H)\big) \cdot (g_3 \cdot H) = (g_1 \cdot H) \cdot \big((g_2 \cdot H) \cdot (g_3 \cdot H)\big)$,

(4) $(g_1 \cdot H) \cdot (g_1^{-1} \cdot H) = H$.

(d) Alors $(G/H, \star, 1 \cdot H)$

$$\star : G/H \times G/H \to G/H, \quad g_1 \cdot H \star g_2 \cdot H := (g_1 \cdot H) \cdot (g_2 \cdot H) = (g_1 \cdot g_2) \cdot H$$

est un groupe (le même que dans la proposition 1.7).

Théorèmes d'isomorphisme

Rappelons qu'un homomorphisme de groupes est injectif si et seulement si son noyau est 'trivial' (c'est-à-dire ne contient que l'élément neutre). Le théorème d'isomorphisme est une généralisation de cette assertion très utile. Nous présentons trois théorèmes d'isomorphisme. Le premier est d'une très grande importance et on l'utilisera beaucoup. En fait, les deux autres théorèmes d'isomorphisme en sont déduits.

Théorème 1.10 (1er théorème d'isomorphisme/Homomorphiesatz)**.** *Soit $\varphi : G \to H$ un homomorphisme de groupes. Soit $N := \ker(\varphi)$ son noyau.*

(a) Pour tout $g \in G$ et tout $n \in N$ on a $\varphi(gn) = \varphi(g)$. Donc pour tout $g_1, g_2 \in gN$ on a $\varphi(g_1) = \varphi(g_2)$. Donc l'image $\varphi(g)$ ne dépend que de la classe gN de g suivant N.

(b) (a) nous permet de définir l'application

$$\overline{\varphi} : G/N \to H, \quad gN \mapsto \overline{\varphi}(gN) := \varphi(g).$$

C'est un homomorphisme injectif de groupes. Donc $\overline{\varphi} : G/N \to \mathrm{im}(\varphi)$ est un isomorphisme de groupes.

(Cette application est la même que dans le théorème 5.19 du cours Structures mathématiques*.)*

Démonstration. (a) C'est clair.
(b)

Homomorphisme $\overline{\varphi}(g_1N \cdot g_2N) = \overline{\varphi}(g_1g_2N) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1N)\overline{\varphi}(g_2N)$.

Injectivité Si $\overline{\varphi}(gN) = \varphi(g) = 1$, alors $g \in N$, donc $gN = N$.

Calcul de l'image Soit $h \in \mathrm{im}(\varphi)$. Donc, il existe $g \in G$ tel que $\varphi(g) = h$, donc $\overline{\varphi}(gN) = \varphi(g) = h$.

□

Exemple 1.11. *(a) On sait déjà que tout noyau d'un homomorphisme de groupes est un sous-groupe distingué. Le théorème d'isomorphisme nous renseigne en plus que l'assertion réciproque est également vraie : tout sous-groupe distingué $H \trianglelefteq G$ est le noyau d'un homomorphisme de groupes : de la projection naturelle modulo H.*

(b) Soient $n \in \mathbb{N}$ et $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection naturelle de noyau $n\mathbb{Z}$. L'application $\overline{\pi} : \mathbb{Z}/\ker(\pi) = \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est l'identité.

(c) Soit $n \in \mathbb{N}_{>1}$. Le noyau $\mathrm{sgn} : S_n \to \{+1, -1\}$ est le groupe alterné A_n et $\overline{\mathrm{sgn}} : S_n/\ker(\mathrm{sgn}) = S_n/A_n \to \{+1, -1\}$ est un isomorphisme.

La proposition suivante est importante car elle décrit les sous-groupes des groupes quotients. Elle peut être comparée avec une proposition du cours d'algèbre linéaire 2 où on donne la classification des sous-espace vectoriels des espaces vectoriels quotients.
D'abord un lemme.

Lemme 1.12. *(a) Soient $\pi : G \to G'$ un homomorphisme de groupes et $U \leq G$ un sous-groupe qui contient $\ker(\pi)$. Alors $\pi^{-1}(\pi(U)) = U$.*

(b) Soient $\pi : G \to G'$ une application surjective entre ensembles et $H \subseteq G'$ un sous-ensemble. Alors $H = \pi(\pi^{-1}(H))$.

Démonstration. (a) « $\subseteq$ » : Soit $x \in \pi^{-1}(\pi(U))$, donc $\pi(x) \in \pi(U)$, donc $\pi(x) = \pi(u)$ pour un $u \in U$. Donc $1 = \pi(x)\pi(u)^{-1} = \pi(xu^{-1})$, donc $xu^{-1} \in \ker(\pi) \subseteq U$, donc $xu^{-1} = v \in U$, donc $x = uv \in U$.
« $\supseteq$ » : Soit $u \in U$, donc $\pi(u) \in \pi(U)$, donc $u \in \pi^{-1}(\pi(U))$.
(b) « $\subseteq$ » : Soit $h \in H$. Comme π est surjectif, il existe $g \in G$ tel que $\pi(g) = h$. Donc $g \in \pi^{-1}(H)$ et $h = \pi(g) \in \pi(\pi^{-1}(H))$.
« $\supseteq$ » : Soit $x \in \pi(\pi^{-1}(H))$. Donc, il existe $g \in \pi^{-1}(H)$ tel que $x = \pi(g)$. Mais, $x = \pi(g)$ appartient à H car $g \in \pi^{-1}(H)$. □

Proposition 1.13. *Soit G un groupe et $N \trianglelefteq G$ un sous-groupe normal et $\pi : G \to G/N$ la projection naturelle.*

(a) L'application

$$\Phi : \{H \mid H \leq G/N \text{ sous-groupe } \} \longrightarrow \{U \mid U \leq G \text{ sous-groupe t.q. } N \subseteq U\},$$

donnée par $H \mapsto \pi^{-1}(H)$ est bijective. L'inverse Ψ de Φ est $U \mapsto \pi(U)$.

(b) Soient $H_1, H_2 \leq G/N$ deux sous-groupes. Alors

$$H_1 \subseteq H_2 \quad \Leftrightarrow \quad \Phi(H_1) \subseteq \Phi(H_2).$$

(c) Soit $H \leq G/N$ un sous-groupe. Alors

$$H \trianglelefteq G/N \quad \Leftrightarrow \quad \Phi(H) \trianglelefteq G.$$

Démonstration. (a)

- Pour $H \leq G/N$ l'image réciproque $\Phi(H) = \pi^{-1}(H)$ est en effet un sous-groupe comme vous l'avez vu dans le cours structures mathématiques. En plus $\pi^{-1}(H) \supseteq \pi^{-1}(\{1\}) = \ker(\pi) = N$.
- Vous avez aussi vu que les images des homomorphismes de groupes sont des sous-groupes du groupe d'arrivée, donc $\Psi(U) = \pi(U)$ est un sous-groupe de G/N.
- Soit $U \leq G$ un sous-groupe tel que $N \subseteq U$. Par le lemme 1.12(a) on a : $\Phi(\Psi(U)) = \pi^{-1}(\pi(U)) = U$.
- Soit $H \leq G/N$ un sous-groupe. Par le lemme 1.12(b) on a : $\Psi(\Phi(H)) = \pi(\pi^{-1}(H)) = H$.

(b) est clair.
(c) Cela est une conséquence directe des deux faits (Proposition 1.4) : l'image réciproque d'un sous-groupe normal est normale ; l'image par un homomorphisme surjectif d'un sous-groupe normal est également normale. □

Remarque 1.14. *(a) Tout sous-groupe $U \subseteq \mathbb{Z}$ est égal à $m\mathbb{Z}$ pour un $m \in \mathbb{N}$.*

Effectivement, si $U = \{0\}$, alors $U = m\mathbb{Z}$ pour $m = 0$. Supposons maintenant $U \neq \{0\}$. Alors $U \cap \mathbb{N}_{>0}$ est un sous-ensemble non-vide des nombres naturels (il est impossible que tout élément de U est non-positif car si $u \in U$ est négatif, $-u$ est positif et appartient à U en tant qu'inverse de u). Donc $U \cap \mathbb{N}_{>0}$ possède un plus petit élément, appelons-le m.

On montrera $U = m\mathbb{Z}$. Comme $m \in U$, l'inclusion $U \supseteq m\mathbb{Z}$ est claire. Pour montrer l'autre inclusion, prenons $u \in U$. On applique la division euclidienne par m pour obtenir

$$u = mq + r \text{ pour un reste } 0 \leq r \leq m - 1.$$

On réécrit cette égalité comme $r = u - mq$ pour obtenir $r \in U$ (car $u \in U$, $-mq \in U$ et U est un sous-groupe). Comme r est strictement plus petit que le plus petit élément positif m de U, il en suit que r ne peut pas être positif. Donc $r = 0$ et en conséquence $u = mq \in m\mathbb{Z}$.

(b) Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}_{\geq 1}$ est de la forme $m\mathbb{Z}/n\mathbb{Z}$ avec $m \mid n$.

Pour le voir, on considère la projection $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Soit $H \subseteq \mathbb{Z}/n\mathbb{Z}$ un sous-groupe. Soit $U = \pi^{-1}(H)$; ce groupe est égal à $m\mathbb{Z}$ pour un $m \in \mathbb{N}$ par (a). Le fait $n\mathbb{Z} \subseteq m\mathbb{Z}$ se traduit en $m \mid n$. Alors $H = m\mathbb{Z}/n\mathbb{Z}$ par la proposition 1.13.

Pour énoncer et démontrer les deux autres théorèmes d'isomorphisme, nous avons d'abord besoin du lemme suivant.

Lemme 1.15. *Soient G un groupe, $H \leq G$ un sous-groupe et $N \leq G$ un sous-groupe normal. Soit $HN := \{hn \mid h \in H, n \in N\}$. Alors :*

(a) $H \cap N$ est un sous-groupe normal de H.

(b) $HN = NH := \{nh \mid h \in H, n \in N\}$

(c) HN *est un sous-groupe de* G*.*

(d) N *est un sous-groupe normal de* HN*.*

(e) Si H *est aussi un sous-groupe normal de* G*, alors* HN *est un sous-groupe normal de* G*.*

Démonstration. Exercice. □

Les deux autres théorèmes d'isomorphisme illustrent très bien comment appliquer le théorème d'isomorphisme. Le schéma est souvent ainsi : Soit $\varphi : G \to H$ une application entre deux groupes.

(1) S'assurer que φ est un homomorphisme de groupes.

(2) Calculer $\mathrm{im}(\varphi)$.

(3) Calculer $\ker(\varphi)$.

Ayant fait cela, le théorème d'isomorphisme nous donne que

$$\varphi : G/\ker(\varphi) \to \mathrm{im}(\varphi)$$

est un isomorphisme de groupes.

Proposition 1.16 (Deuxième théorème d'isomorphisme)**.** *Soient* G *un groupe,* $H \leq G$ *un sous-groupe et* $N \leq G$ *un sous-groupe normal. Alors, l'homomorphisme naturel de groupes*

$$\varphi : H \to HN \to HN/N, \quad h \mapsto hN$$

« induit » (par le théorème d'isomorphisme 1.10) l'isomorphisme de groupes

$$\overline{\varphi} : H/(H \cap N) \to HN/N, \quad h(H \cap N) \mapsto hN.$$

Démonstration. Noter d'abord que le lemme 1.15 nous assure que tout est bien défini. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $h \in H$ tels que $hN = N$, donc $h \in H \cap N$, montrant $\ker(\varphi) = H \cap N$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 1.10. □

Proposition 1.17 (Troisième théorème d'isomorphisme)**.** *Soient* G *un groupe,* $H, N \lhd G$ *des sous-groupes normaux tels que* $N \subseteq H$*. Alors, l'homomorphisme naturel de groupes*

$$\varphi : G/N \to G/H, \quad gN \mapsto gH$$

« induit » (par le théorème d'isomorphisme 1.10) l'isomorphisme de groupes

$$\overline{\varphi} : (G/N)/(H/N) \to G/H, \quad gN(H/N) \mapsto gH.$$

Démonstration. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $gN \in G/N$ tels que $gH = H$, donc $g \in H$, donc $gN \in H/N$, montrant $\ker(\varphi) = H/N$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 1.10. □

2 Homomorphismes et isomorphismes d'anneaux

Objectifs :

- Apprendre et maîtriser la notion d'idéal ;
- connaître la définition de quotients d'un anneau par un idéal ;
- savoir calculer dans les quotients ;
- connaître et savoir appliquer les théorèmes d'isomorphisme ;
- savoir démontrer des propriétés simples.

Homomorphismes

Rappelons l'idée principale derrière la définition des homomorphismes : ce sont des applications qui préservent toutes les structures. Ici on voudra définir les homomorphismes d'anneaux : on exigera donc qu'ils preservent $+, \cdot$ ainsi que les éléments neutres pour $+$ et $\cdot$.

Définition 2.1. *Soient* $(A, +, \cdot, 0, 1)$ *et* $(A', +', \cdot', 0', 1')$ *deux anneaux. On appelle* (homo)morphisme d'anneaux *toute application*

$$\varphi : A \to A'$$

telle que

- φ *est un homomorphisme de groupes de* $(A, +, 0)$ *dans* $(A', +', 0')$*, c'est-à-dire* $\forall\, a, b \in A :\ \varphi(a + b) = \varphi(a) +' \varphi(b)$*,*
- $\forall\, a, b \in A :\ \varphi(a \cdot b) = \varphi(a) \cdot' \varphi(b)$ *et*
- $\varphi(1) = 1'$.

On utilise la notation $\mathrm{Hom}(A, A')$ *pour l'ensemble des homomorphismes d'anneaux de* A *dans* A'*.*
Si A *et* A' *sont des corps, on parle aussi d'un* homomorphisme de corps*.*
Tout homomorphisme bijectif est appelé isomorphisme*, tout homomorphisme injectif est appelé* monomorphisme *et tout homomorphisme surjectif est appelé* épimorphisme

La propriété $\varphi(0) = 0$ est toujours satisfaite car $(A, +, 0)$ est un groupe comme nous l'avons vu dans le lemme 0.10. Par contre, $\varphi(1) = 1'$ n'est en général pas une conséquence des deux premières propriétés (par exemple, l'homomorphisme qui envoie tout élément sur 0 vérifie les deux premières propriétés).
Après cette définition, nous allons utiliser les notations $0, 1, +, \cdot$ pour tout anneau.

Exemple 2.2.

- *L'inclusion* $\varphi : \mathbb{Z} \to \mathbb{Q}$*,* $n \mapsto \frac{n}{1}$ *est un homomorphisme d'anneaux.*
- *L'inclusion* $\varphi : \mathbb{R} \to \mathrm{Mat}_n(\mathbb{R})$*,* $a \mapsto \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$ *est un homomorphisme d'anneaux.*
- *Soit* $n \in \mathbb{N}_{>0}$*. L'application* $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$*,* $a \mapsto \overline{a} = a + n\mathbb{Z}$*, est un homomorphisme d'anneaux.*

Lemme 2.3. *L'inverse de tout isomorphisme d'anneaux est aussi un isomorphisme d'anneaux.*

Démonstration. Exercice. □

Définition 2.4. *Soit A un anneau commutatif. On appelle* A-algèbre *tout anneau B muni d'un homomorphisme d'anneaux $\varphi : A \to B$ tel que pour tout $a \in A$ et tout $b \in B$ on a $\varphi(a) \cdot b = b \cdot \varphi(a)$.*

Ce que nous appelons « algèbre » s'appelle souvent plus précisement « algèbre associative (unitaire) ».

Exemple 2.5. *Soient $n \in \mathbb{N}_{>0}$, $(K, +, \cdot, 0, 1)$ un corps (commutatif!) et $\varphi : K \to \mathrm{Mat}_n(K)$, $a \mapsto \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix}$. Alors, $(\mathrm{Mat}_n(K), \varphi)$ est une K-algèbre.*

Noyaux

Définition 2.6. *Soient $(A_1, +, \cdot, 0, 1)$ et $(A_2, +, \cdot, 0, 1)$ des anneaux et $\varphi : A_1 \to A_2$ un homomorphisme d'anneaux. Le* noyau de φ *est défini comme*

$$\ker(\varphi) := \{a \in A_1 \mid \varphi(a) = 0\}.$$

Noter que l'homomorphisme d'anneaux φ est automatiquement un homomorphisme de groupes de $(A_1, +, 0)$ dans $(A_2, +, 0)$ et $\ker(\varphi)$ est précisement le noyau de cet homomomorphisme de groupes.

La proposition suivante est l'analogue pour les anneaux de la proposition 0.16 pour les groupes.

Proposition 2.7. *Nous avons l'équivalence :*

$$\varphi \text{ est injectif } \Leftrightarrow \ker(\varphi) = \{0\}.$$

Démonstration. Il suffit de noter que tout homomorphisme d'anneaux est aussi un homomorphisme de groupes. □

Exemple 2.8. *Soit $n \in \mathbb{N}_{>0}$. Nous considérons encore l'homomorphisme d'anneaux*

$$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad a \mapsto \overline{a} = a + n\mathbb{Z}.$$

Nous avons

$$\ker(\varphi) = n\mathbb{Z}.$$

Sous-anneaux et idéaux

Définition 2.9. *Soit A un anneau commutatif. On appelle* sous-anneau de A *tout sous-ensemble $B \subseteq A$ tel que*

- *$(B, +, 0)$ est un sous-groupe de $(A, +, 0)$ (alors, il n'est pas vide et pour tout $b_1, b_2 \in B$, on a $b_1 - b_2 \in B$),*
- *pour tout $b_1, b_2 \in B$ on a $b_1 \cdot b_2 \in B$ et*

- $1 \in B$.

L'exemple fondamental d'un sous-anneau est l'image d'un homomorphisme d'anneaux. En fait, tout sous-anneau peut être vu comme l'image d'un homomorphisme d'anneaux : l'inclusion.

Proposition 2.10. *Soient A_1, A_2 des anneaux commutatifs et $\varphi : A_1 \to A_2$ un homomorphisme d'anneaux. Alors $\varphi(A_1) = \mathrm{im}(\varphi)$ est un sous-anneau de A_2.*

Démonstration. Nous savons que $\mathrm{im}(\varphi)$ est un sous-groupe de A_2. En plus, $\varphi(1) = 1$ implique $1 \in \mathrm{im}(\varphi)$. Soient $b_1, b_2 \in \mathrm{im}(\varphi)$. Par définition de l'image, on peut écrire $b_1 = \varphi(a_1)$ et $b_2 = \varphi(a_2)$ avec $a_1, a_2 \in A$. Donc, $b_1 b_2 = \varphi(a_1)\varphi(a_2) = \varphi(a_1 a_2) \in \mathrm{im}(\varphi)$. □

Nous allons maintenant définir un autre type de sous-objet d'un anneau : l'idéal, qui jouera le même rôle pour les anneaux que les sous-groupes normaux jouent pour les groupes.

Définition 2.11. *Soit A un anneau commutatif. On appelle* idéal de A *tout sous-ensemble $I \subseteq A$ tel que*

- *$(I, +, 0)$ est un sous-groupe de $(A, +, 0)$ (alors, il n'est pas vide et pour tout $i_1, i_2 \in I$, on a $i_1 - i_2 \in I$) et*
- *pour tout $i \in I$ et tout $a \in A$ on a $a \cdot i \in I$.*

Notation : $I \trianglelefteq A$.

Pour montrer qu'un sous-ensemble $I \subseteq A$ est un idéal il suffit de montrer :

- $\forall\, i_1, i_2 \in I : i_1 + i_2 \in I$ et
- $\forall\, i \in I, \forall\, a \in A : a \cdot i \in I$.

Effectivement, la condition $i_1 - i_2 \in I$ provient de $i_1 + (-1 \cdot i_2) \in I$.

Remarque 2.12. *Si A n'est pas commutatif, la définition que nous avons donnée est celle d'un* idéal à gauche. *La manière de définir les idéaux à droite est évidente (remplacer $a \cdot i \in A$ par $i \cdot a \in A$ dans la dernière condition); on a aussi la notion d'idéal bilatère. Dans ce cours nous allons utiliser uniquement les idéaux pour les anneaux commutatifs, comme dans la définition précédente.*

Exemple 2.13. *(a) Tout anneau A possède les idéaux $\{0\}$ et A.*

(b) $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ pour tout $n \in \mathbb{Z}$.

(c) Soit A un anneau. Tout élément $b \in A$ donne l'idéal principal engendré par *b, c'est-à-dire, l'ensemble des multiples de b :*

$$(b) := Ab = A \cdot b = \{ab \mid a \in A\}.$$

Lemme 2.14. *Soient A un anneau commutatif et $I \trianglelefteq A$ un idéal.*

(a) Si I contient une unité $u \in A^\times$, alors $I = A$.

(b) Un idéal $I \trianglelefteq A$ n'est pas un sous-anneau sauf si $I = A$.

(c) Si A est un corps, alors les seuls idéaux sont $\{0\}$ et A.

Démonstration. (a) Comme u est une unité, il existe $v \in A$ tel que $vu = 1$. Soit $a \in A$. Alors, $a = a \cdot 1 = avu = (av)u \in I$.
(b) Si I est un sous-anneau, alors $1 \in I$, et cela implique $I = A$.
(c) Soit $I \neq \{0\}$ un idéal de A. On applique (a) avec n'importe quel $0 \neq u \in I$ qui est une unité parce que tous les éléments non-nuls d'un corps sont des unités. □

L'exemple fondamental d'un idéal est le noyau d'un homomorphisme d'anneaux. En fait, nous verrons bientôt que tout idéal normal est le noyau d'un homomorphisme d'anneaux.

Proposition 2.15. *Soit $\varphi : A_1 \to A_2$ un homomorphisme d'anneaux. Alors, le* noyau de φ *est un idéal de A_1.*

Démonstration. Nous savons déjà que $\ker(\varphi)$ est un sous-groupe. Il suffit donc de montrer qu'il est préservé par la multiplication par $a \in A$. Soit $i \in \ker(\varphi)$, donc $\varphi(i) = 0$. Nous avons

$$\varphi(ai) = \varphi(a)\varphi(i) = \varphi(a) \cdot 0 = 0,$$

donc $ai \in \ker(\varphi)$. □

Lemme 2.16. *Soient A un anneau commutatif et $I, J, K \trianglelefteq A$ des idéaux. Alors :*

(a) $I \cap J$ est un idéal de A.

(b) $I + J := \{i + j \mid i \in I, j \in J\}$ est un idéal de A.

(c) $I \cdot J := \{\sum_{\ell=1}^{r} i_\ell j_\ell \mid r \in \mathbb{N}, i_\ell \in I, j_\ell \in J\}$ est un idéal de A.

(d) $I + J = J + I$.

(e) $(I \cdot J) \cdot K = I \cdot (J \cdot K)$.

(f) $I \cdot (J + K) = I \cdot J + I \cdot K$.

Démonstration. Exercice. □

Lemme 2.17. *Soient A un anneau commutatif, $B \leq A$ un sous-anneau et $I, J \trianglelefteq A$ des idéaux. Alors :*

(a) $B \cap I$ est un idéal de B.

(b) $B + I := \{b + i \mid b \in B, i \in I\}$ est un sous-anneau de A.

(c) I est un idéal de $B + I$.

Démonstration. Exercice. □

Quotients d'anneaux

Soit $(A, +, \cdot, 0, 1)$ et $I \trianglelefteq A$ un idéal. Comme $(A, +, 0)$ est un groupe abélien, le sous-groupe $I \leq A$ est normal. On considère le groupe quotient $(A/I, +, 0 + I)$ qui résulte de la proposition 1.7 et notre but est de définir une multiplication

$$\otimes : A/I \times A/I \to A/I$$

telle que $(A/I, +, \cdot, 0 + I, 1 + I)$ est un anneau.
Soient $a, a', b, b' \in A$ tels que

$$a' - a \in I \quad \text{et} \quad b' - b \in I.$$

Il existe donc $i, j \in I$ tels que $a' = a + i$ et $b' = b + j$; donc

$$a'b' = (a + i)(b + j) = ab + aj + bi + ij.$$

Nous voulons $a'b' - ab \in I$. Ceci est clairement satisfait car I est un idéal ! Donc supposons cela. On l'applique comme avant :

> Soient a et a' deux représentants de la même classe, c'est-à-dire $a' + I = a + I$; soient b et b' aussi dans la même classe : $b' + I = b + I$.
>
> Alors $a'b'$ et ab représentent aussi la même classe : $a'b' + I = ab + I$.

Cela veut dire : *la classe $ab + I$ ne dépend que de la classe de a et de la classe de b.* Ceci nous permet de faire la définition recherchée :

$$(a + I) \cdot (b + I) := ab + I.$$

Plus précisément nous avons la proposition suivante :

Proposition 2.18. *Soient $(A, +, \cdot, 0, 1)$ un anneau commutatif et $I \trianglelefteq A$ un idéal. Avec les définitions ci-dessus nous avons :*

(a) $(A/I, \oplus, \otimes, 0 + I, 1 + I)$ *est un anneau commutatif, appelé* (anneau) quotient de A par I.

(b) L'application

$$\pi : A \to A/I, \quad a \mapsto a + I$$

est un homomorphisme d'anneaux surjectif, appelé projection naturelle. *On a* $\ker(\pi) = I$.

Démonstration. Comme nous savons déjà par la proposition 1.7 que $(A/I, \oplus, 0 + I)$ est un groupe abélien, il ne reste que peu de vérifications à faire qui sont l'objet d'un exercice. □

Exemple 2.19. *L'exemple le plus important que nous connaissons pour l'instant est $\mathbb{Z}/n\mathbb{Z}$; noter que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$!*

Remarque 2.20. *Si l'anneau n'est pas commutatif, on peut quand même construire un quotient si l'idéal I est bilatère. On ne le fera pas dans ce cours.*

Proposition 2.21. *Soit A un anneau et $I \trianglelefteq A$ un idéal et $\pi : A \to A/I$ la projection naturelle. Alors, l'application*

$$\Phi : \{J \mid J \trianglelefteq A/I \text{ idéal}\} \longrightarrow \{K \mid K \trianglelefteq A \text{ idéal tel que } I \subseteq K\},$$

donnée par $J \mapsto \pi^{-1}(J)$ est bijective. L'inverse de Φ est $K \mapsto \pi(K)$.

Démonstration. Exercice. □

Théorèmes d'isomorphisme

Théorème 2.22 (1er théorème d'isomorphisme/Homomorphiesatz)**.** *Soit $\varphi : A \to B$ un homomorphisme d'anneaux commutatifs. Soit $N := \ker(\varphi)$ son noyau. L'application*

$$\overline{\varphi} : A/N \to \operatorname{im}(\varphi) \subseteq B, \quad a + N \mapsto \overline{\varphi}(a + N) := \varphi(a)$$

provenant du cas des groupes (théorème 1.10) est un isomorphisme d'anneaux.

Démonstration. On sait déjà que $\overline{\varphi}$ est un isomorphisme de groupes. Donc il suffit de démontrer que c'est un homomorphisme d'anneaux :

- $\overline{\varphi}(1 + N) = \varphi(1) = 1$.
- $\overline{\varphi}((a + N) \otimes (b + N)) = \overline{\varphi}(a \cdot b + N) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \overline{\varphi}(a + N) \cdot \overline{\varphi}(b + N)$.

□

Proposition 2.23 (Deuxième théorème d'isomorphisme)**.** *Soient A un anneau commutatif, $B \leq A$ un sous-anneau et $I \trianglelefteq A$ un idéal. Alors, l'homomorphisme naturel d'anneaux*

$$\varphi : B \to (B + I)/I, \quad b \mapsto b + I,$$

« induit » (par le théorème d'isomorphisme 2.22) l'isomorphisme d'anneaux

$$\overline{\varphi} : B/(B \cap I) \to (B + I)/I, \quad b + (B \cap I) \mapsto b + I.$$

Démonstration. Noter d'abord que le lemme 2.17 nous assure que tout est bien défini. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $b \in B$ tels que $b + I = I$, donc $b \in B \cap I$, montrant $\ker(\varphi) = B \cap I$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 2.22. □

Proposition 2.24 (Troisième théorème d'isomorphisme)**.** *Soient A un anneau commutatif et $I, J \trianglelefteq A$ des idéaux tels que $J \subseteq I$. Alors, l'homomorphisme naturel d'anneaux*

$$\varphi : A/J \to A/I, \quad a + J \mapsto a + I$$

« induit » (par le théorème d'isomorphisme 2.22) l'isomorphisme d'anneaux

$$\overline{\varphi} : (A/J)/(I/J) \to A/I, \quad a + J + (I/J) \mapsto a + I.$$

Démonstration. L'homomorphisme φ est visiblement surjectif et son noyau est composé des éléments $a + J \in A/J$ tels que $a + I = I$, donc $a \in I$, donc $a + J \in I/J$, montrant $\ker(\varphi) = I/J$. L'existence de $\overline{\varphi}$ résulte donc d'une application directe du théorème d'isomorphisme 2.22. □

3 Anneaux euclidiens

Objectifs :

- Maîtriser l'anneau des polynômes, la division euclidienne, son algorithme d'Euclide et la propriété universelle des polynômes ;
- connaître la définition d'anneau euclidien et savoir l'expliquer en tant que généralisation des entiers relatifs et de l'anneau des polynômes à coefficients dans un corps ;
- connaître et savoir appliquer l'algorithme d'Euclide dans un anneau euclidien ;
- connaître la définition des pgcd et ppcm et savoir les calculer dans un anneau euclidien général ;
- savoir calculer des relations de Bézout ;
- savoir démontrer des propriétés simples.

A partir d'ici, nous supposons que tout anneau est commutatif, sauf si le contraire est explicitement mentionné.

Dans le cours « structures mathématiques » nous avons vu l'importance de la division euclidienne pour les entiers relatifs. Il existe aussi une division euclidiennes pour les polynômes que nous avons utilisé dans le cours « algèbre linéaire 2 ». Nous commençons cette section par quelques notes sur les polynômes avant de prendre les entiers relatifs et les polynômes comme modèle pour introduire une nouvelle structure qui les unifie : celle des anneaux euclidiens.

Polynômes

Définition 3.1. *Soit A un anneau.*

- *Un* polynôme à coefficients dans A *(pour la variable X) est une « somme formelle » $\sum_{i=0}^{n} a_i X^i$ où $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in A$.*

  Ici, X n'est qu'un symbole. Nous pouvons le remplacer par tout autre symbole, par exemple Y, x, t, T, etc.

  On comprends $a_m = 0$ pour tout $m > n$.

- *(Définition plus formelle :) Un* polynôme à coefficients dans A *est une application $a : \mathbb{N} \to A$ telle qu'il existe $n \in \mathbb{N}$ tel que pour tout $m > n$ on a $a(m) = 0$.*

  Si a est une telle application, nous écrivons $\sum_{i=0}^{n} a(i) X^i$.

- *Nous notons $A[X]$ l'ensemble de tous les polynômes à coefficients dans A pour la variable X.*

- *Soit $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$. Le* degré *de f (notation : $\deg(f)$) est l'entier m maximal tel que $a_m \neq 0$. Si $f = 0$, alors on pose $\deg(f) = -\infty$. On appelle $a_d X^d$ avec $d = \deg(f)$ le* monôme dominant *de f. On appelle f* unitaire (anglais : monic ; allemand : normiert) *si $a_{\deg(f)} = 1$.*

- *Soient* $f(X) = \sum_{i=0}^{n} a_i X^i$ *et* $g(X) = \sum_{j=0}^{m} b_i X^i$ *deux éléments de* $A[X]$. *Nous définissons la* somme *de ces deux polynômes comme :*

$$f(X) + g(X) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i,$$

où on suppose $a_i = 0$ *si* $i > n$ *et* $b_j = 0$ *si* $j > m$.

- *Soient* $f(X) = \sum_{i=0}^{n} a_i X^i$ *et* $g(X) = \sum_{j=0}^{m} b_i X^i$ *deux éléments de* $A[X]$. *Nous définissons le* produit *de ces deux polynômes comme :*

$$f(X) \cdot g(X) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k,$$

où on suppose $a_i = 0$ *si* $i > n$ *et* $b_j = 0$ *si* $j > m$.

Remarque 3.2. *Il faut bien faire la différence entre un polynôme et la fonction qu'il représente : par exemple pour* $A = \mathbb{F}_2$, *les polynômes* $f(X) = X$ *et* $g(X) = X^3$ *sont différents, mais,* $f(b) = b = g(b)$ *pour tout* $b \in \mathbb{F}_2$, *donc vus comme des fonctions* $\mathbb{F}_2 \to \mathbb{F}_2$ *ils sont égaux !*

Proposition 3.3. *Soit* A *un anneau commutatif. Alors,* $(A[X], +, \cdot, 0, 1)$ *est un anneau commutatif.*

Démonstration. La vérification est facile. On ne la fera pas. □

Proposition 3.4. *Soient* A *un anneau et* $f, g \in A[X]$.

(a) $\deg(f + g) \leq \max(\deg(f), \deg(g))$ et $\deg(fg) \leq \deg(f) + \deg(g)$.

(b) Soient $f(X) = \sum_{i=0}^{n} a_i X^i$ *et* $g(X) = \sum_{j=0}^{m} b_i X^i$ *où on suppose* $n = \deg(f)$ *et* $m = \deg(g)$. *Si l'une des conditions*

(1) $a_n b_m \neq 0$;

(2) $a_n \in A^\times$ *ou* $b_m \in A^\times$;

(3) A *est un anneau intègre ;*

est satisfaite, alors $\deg(fg) = \deg(f) + \deg(g)$.

Démonstration. (a) Cela ressort de la définition de la somme et du produit de deux polynômes. Mais, notez que si $f = 0$, nous devons faire le calcul $-\infty + \deg(g) = -\infty$; donc, nous calculons avec le symbole ∞ d'une façon naïve (sans en donner un traitement formel).
(b) La première condition implique que $a_n b_m X^{n+m}$ est le monôme dominant de $f \cdot g$. Les deux autres conditions nous ramènent directement à la première. □

Corollaire 3.5. *Soit* A *un anneau intègre.*

(a) $(A[X])^\times = A^\times$. *C'est-à-dire que les seules unités de* $A[X]$ *sont les polynômes constants où la constante est une unité de* A.

(b) $A[X]$ est intègre.

Démonstration. (a) Il est clair que les polynômes constants où la constante est une unité de A appartiennent à $(A[X])^\times$. Soit $f(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme de degré n dans $(A[X])^\times$. Alors par définition il existe $g(X) = \sum_{j=0}^{m} b_i X^i$ (on suppose $m = \deg(g)$) tel que $f(X)g(X) = 1$ (polynôme constant). Par la proposition 3.4 nous obtenons $n+m = 0$. Comme $n, m \geq 0$ (il est clair que f et g ne sont pas égaux au polynôme constant 0), on en conclut $n = m = 0$, alors $f(X) = a_0$ et $g(X) = b_0$. L'égalité $1 = a_0 b_0$ montre $f = a_0 \in A^\times$.
(b) Si $fg = 0$, alors $-\infty = \deg(f) + \deg(g)$ par la proposition 3.4, dont nous concluons $f = 0$ ou $g = 0$. □

Nous rappelons la division euclidienne.

Théorème 3.6 (Division euclidienne)**.** *Soient A un anneau commutatif et $g = \sum_{i=0}^{d} b_i X^i \in A[X]$ un polynôme de degré $d \geq 0$. On suppose $b_d \in A^\times$ (cette hypothèse est automatiquement satisfaite si A est un corps).*
Alors, pour tout polynôme $f \in A[X]$ il existe des uniques polynômes $q, r \in A[X]$ tels que

$$f = qg + r \quad \text{et} \quad \deg(r) < d.$$

Démonstration. La démonstration a été donné au cours « algèbre linéaire 2 ». Nous n'allons pas la redonner en classe.
Soit $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré n.
Existence : Nous montrons l'existence par récurrence sur n. Si $n < d$, on pose $q = 0$ et $r = f$ et on a terminé. Supposons donc $n \geq d$ et que l'existence est déjà connue pour tous les polynômes de degré strictement plus petit que n. On pose

$$f_1(X) := f(X) - a_n \cdot b_d^{-1} X^{n-d} g(X).$$

C'est un polynôme de degré au plus $n-1$ parce que nous avons annulé le coefficient devant X^n. Alors, par hypothèse de récurrence il existe $q_1, r_1 \in A[X]$ tels que $f_1 = q_1 g + r_1$ et $\deg(r_1) < d$. Donc

$$f(X) = f_1(X) + a_n b_d^{-1} g(X) X^{n-d} = q(X)g(X) + r_1(X)$$

où $q(X) := q_1(X) + a_n b_d^{-1} X^{n-d}$ et nous avons démontré l'existence.
Unicité : Supposons $f = qg + r = q_1 g + r_1$ avec $q, q_1, r, r_1 \in A[X]$ et $\deg(r), \deg(r_1) < d$. Alors $g(q - q_1) = r_1 - r$. Si $q = q_1$, alors $r = r_1$ et on a terminé. Si $q \neq q_1$, alors $\deg(q - q_1) \geq 0$ et par la proposition 3.4(b) on trouve $\deg(r_1 - r) = \deg(g(q - q_1)) \geq \deg(g) = d$. Cela contredit la proposition 3.4, donc $q \neq q_1$ ne peut pas apparaître. □

Nous allons voir tout de suite que la division euclidienne nous permet de généraliser l'algorithme d'Euclide pour le calcul d'un pgcd.

Evaluation et propriété universelle des polynômes

Ici on continue d'abord par l'évaluation de polynômes en une valeur.

Définition 3.7. *Soit A un anneau. Soit B aussi un anneau qui contient A comme sous-anneau : $A \subseteq B$. Soit $b \in B$. On appelle* évaluation en b *l'application*

$$\mathrm{ev}_b : A[X] \to B, \quad f(X) = \sum_{i=0}^{d} a_i X^i \mapsto f(b) = \sum_{i=0}^{d} a_i b^i.$$

Exemple 3.8. *Soient $A = B = \mathbb{Q}$ et $b = 2$. Alors, l'évaluation en 2 est l'application*

$$\mathrm{ev}_2 : \mathbb{Q}[X] \to \mathbb{Q}, \quad f(X) \mapsto f(2).$$

En particulier, $\mathrm{ev}_2(X + 3) = 2 + 3 = 5$.

L'application ev_b de la définition 3.7 est un homomorphisme d'anneaux (même de A-algèbres). Cela est un cas spécial de la proposition suivante qui s'appelle « propriété universelle » de l'anneau des polynômes. Pour voir l'application comme cas spécial, on prend φ comme l'inclusion du sous-anneau A dans B.

Proposition 3.9. *Soient A, B des anneaux, $\varphi : A \to B$ un homomorphisme d'anneaux et $b \in B$. Alors il existe un unique homomorphisme d'anneaux*

$$\Phi : A[X] \to B$$

qui a les propriétés

- $\Phi(X) = b$ *et*
- $\Phi(a) = \varphi(a)$ *pour tout $a \in A$.*

Dans ce cas nous avons pour $f = \sum_{i=0}^{n} a_i X^i$

$$\Phi(f) = \sum_{i=0}^{n} \varphi(a_i) b^i.$$

En particulier, $\mathrm{im}(\Phi) = \Phi(A[X]) \subseteq B$ *est un sous-anneau.*

Démonstration. **Unicité :** Si un tel Φ existe, il doit satisfaire

$$\Phi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \Phi(a_i)\Phi(X)^i = \sum_{i=0}^{n} \varphi(a_i) b^i$$

par les propriétés des homomorphismes d'anneaux. Donc, si un tel Φ existe, il est nécessairement unique.

Existence : On définit

$$\Phi(\sum_{i=0}^{n} a_i X^i) := \sum_{i=0}^{n} \varphi(a_i) b^i$$

pour tout polynôme $\sum_{i=0}^{n} a_i X^i \in A[X]$. Nous devons montrer qu'avec cette définition Φ est un homomorphisme d'anneaux :

- $\Phi(1) = \varphi(1) = 1$.
- $\Phi(f+g) = \Phi(\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{m} c_j X^j) = \Phi(\sum_{i=0}^{\max(n,m)} (a_i + c_i) X^i)$
  $= \sum_{i=0}^{\max(n,m)} \varphi(a_i + c_i) b^i = \sum_{i=0}^{n} \varphi(a_i) b^i + \sum_{j=0}^{m} \varphi(c_j) b^j$
  $= \Phi(\sum_{i=0}^{n} a_i X^i) + \Phi(\sum_{j=0}^{m} c_j X^j) = \Phi(f) + \Phi(g)$.
- $\Phi(f \cdot g) = \Phi((\sum_{i=0}^{n} a_i X^i) \cdot (\sum_{j=0}^{m} c_j X^j)) = \Phi(\sum_{k=0}^{n+m} (\sum_{i=0}^{k} a_i c_{k-i}) X^k)$
  $= \sum_{k=0}^{n+m} \varphi(\sum_{i=0}^{k} a_i c_{k-i}) b^k = (\sum_{i=0}^{n} \varphi(a_i) b^i) \cdot (\sum_{j=0}^{m} \varphi(c_j) b^j)$
  $= \Phi(\sum_{i=0}^{n} a_i X^i) \cdot \Phi(\sum_{j=0}^{m} c_j X^j) = \Phi(f) \cdot \Phi(g)$.

La dernière assertion provient juste du fait général que l'image de tout homomorphisme d'anneaux est un sous-anneau. □

Exemple 3.10. *Soit $i = \sqrt{-1} \in \mathbb{C}$. Par la proposition 3.9, l'évaluation en i est le homomorphisme d'anneaux*

$$\mathrm{ev}_i : \mathbb{Q}[X] \to \mathbb{C}, \quad \mathrm{ev}_i(f) = \sum_{k=0}^{n} a_k i^k = \sum_{k=0,\ \text{pair}}^{n} (-1)^{k/2} a_k + i\Big(\sum_{k=0,\ \text{impair}}^{n} (-1)^{(k-1)/2} a_k\Big).$$

Alors, $\mathrm{im}(\mathrm{ev}_i) = \{a + ib \mid a, b \in \mathbb{Q}\}$ *est un sous-anneau de $\mathbb{C}$, qu'on note $\mathbb{Q}[i]$. C'est même un sous-corps de $\mathbb{C}$, car tout élément non nul possède un inverse :*

$$(a+ib) \cdot \Big(\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}\Big) = 1.$$

On peut remplacer $\mathbb{Q}$ par $\mathbb{Z}$ pour obtenir l'anneau intègre $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ (qui n'est pas un corps, mais un anneau euclidien – définition à venir).

Généralisation : anneau euclidien

Nous connaissons deux anneaux dans lesquels il existe une division euclidienne : les entiers relatifs et l'anneau des polynômes à coefficients dans un corps. Donc, ces deux anneaux – qui de loin semblent être très différents – ont cette propriété importante en commun.
Ici nous allons faire une étape importante d'abstraction : nous formalisons l'idée de la division euclidienne et nous prenons l'idée abstraite comme base pour la définition d'une nouvelle classe d'anneaux : les anneaux euclidiens.
Nous allons aussi voir que dans les anneaux euclidiens, (l'analogue de) l'algorithme d'Euclide nous permet de calculer des plus grands diviseurs communs, des plus petits multiples communs et des identités de Bézout.

Nous comparons maintenant la division euclidienne dans $\mathbb{Z}$ et $K[X]$ où K est un corps.

$\mathbb{Z}$	$K[X]$
Pour tout $a, b \in \mathbb{Z}$, $b \neq 0$	Pour tout $a, b \in K[X]$, $b \neq 0$
$\exists\ q, r \in \mathbb{Z}$ t.q.	$\exists\ q, r \in K[X]$ t.q.
$a = bq + r$ et	$a = bq + r$ et
$\lvert r\rvert < \lvert b\rvert$	$\deg(r) < \deg(b)$

Nous avons pris la définition $\deg(0) = -\infty$ pour que la formule $\deg(fg) = \deg(f) + \deg(g)$ soit toujours correcte (si les coefficients sont dans un anneau intègre ou un corps). On pourrait trouver

cette convention gênante ; on peut s'en passer par l'équivalence :

$$\deg(r) < \deg(b) \Leftrightarrow (r = 0 \text{ ou } \deg(r) < \deg(b)) .$$

On peut donc remplacer la dernière règle pour obtenir :

$\mathbb{Z}$	$K[X]$
Pour tout $a, b \in \mathbb{Z}$, $b \neq 0$	Pour tout $a, b \in K[X]$, $b \neq 0$
$\exists\, q, r \in \mathbb{Z}$ t.q.	$\exists\, q, r \in K[X]$ t.q.
$a = bq + r$ et	$a = bq + r$ et
($r = 0$ ou $\lvert r\rvert < \lvert b\rvert$)	($r = 0$ ou $\deg(r) < \deg(b)$)

Nous voyons que toutes les règles sont les mêmes sauf une partie de la dernière. Qu'est-ce que la valeur absolue d'un entier et le degré d'un polynôme ont en commun ? Ce sont tous les deux des « mesures de taille » ! On peut et doit être plus précis :

$\mathbb{Z}$	$K[X]$
Pour tout $0 \neq r \in \mathbb{Z}$	Pour tout $0 \neq r \in K[X]$
$\lvert r\rvert$ est un nombre naturel	$\deg(r)$ est un nombre naturel

Donc, $|\cdot|$ (pour $A := \mathbb{Z}$) et $\deg$ (pour $A := K[X]$) sont des applications de la forme $\delta : A \setminus \{0\} \to \mathbb{N}_{\geq 0}$. Nous ajoutons la formalisation dans une troisième colonne.

$\mathbb{Z}$	$K[X]$	A
Pour tout $a, b \in \mathbb{Z}$, $b \neq 0$	Pour tout $a, b \in K[X]$, $b \neq 0$	Pour tout $a, b \in A$, $b \neq 0$
$\exists\, q, r \in \mathbb{Z}$ t.q.	$\exists\, q, r \in K[X]$ t.q.	$\exists\, q, r \in A$ t.q.
$a = bq + r$ et	$a = bq + r$ et	$a = bq + r$ et
($r = 0$ ou $\lvert r\rvert < \lvert b\rvert$)	($r = 0$ ou $\deg(r) < \deg(b)$)	($r = 0$ ou $\delta(r) < \delta(b)$)

La formalisation dans la troisième colonne devient notre définition d'un anneau euclidien :

Définition 3.11. *On appelle* anneau euclidien *tout anneau intègre A tel qu'il existe une application*

$$\delta : A \setminus \{0\} \to \mathbb{N}_{\geq 0}$$

satisfaisant que pour tout $a, b \in A$ avec $b \neq 0$ il existe $q, r \in A$ qui satisfont

$$a = bq + r \quad \text{et} \quad (r = 0 \text{ ou } \delta(r) < \delta(b)).$$

Exemple 3.12.

- *$\mathbb{Z}$ est un anneau euclidien avec $\delta(n) := |n|$ pour $n \in \mathbb{Z} \setminus \{0\}$.*
- *$K[X]$ (pour K un corps) est un anneau euclidien avec $\delta(f) := \deg(f)$ pour $f \in K[X] \setminus \{0\}$.*
- *$\mathbb{Z}[i] := \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ est un anneau euclidien avec $\delta(a + ib) := a^2 + b^2$ pour $a + ib \in \mathbb{Z}[i] \setminus \{0\}$ (exercice).*

Rappelons la définition du plus grand diviseur commun dans $\mathbb{Z}$ du cours « structures mathématiques » :

Définition 3.13. *On appelle* plus grand diviseur commun de $x, y \in \mathbb{Z}$ (notation : $\mathrm{pgcd}(x, y)$) *tout $d \in \mathbb{Z}$ tel que*

- *$d \mid x$ et $d \mid y$ et*

- *pour tout* $e \in \mathbb{Z}$ *on a* $((e \mid x$ *et* $e \mid y) \Rightarrow e \mid d)$.

En fait, on a fait un très petit changement : dans le cours « structures mathématiques » nous avons imposé que d (et e) soit dans $\mathbb{N}$. Comme on veut faire une généralisation aux anneaux généraux, on ne peut pas utiliser $\mathbb{N}$. Avec la définition ci-dessus, 4 et -4 sont tous les deux des plus grands diviseurs communs de 8 et 12. En fait, si d est un plus grand commun diviseur de deux entiers, alors $-d$ l'est aussi. Donc le plus grand diviseur commun de deux entiers n'est pas unique : si on a l'un, on obtient l'autre en multipliant le premier par l'unité -1.
Nous généralisons maintenant la définition du plus grand diviseur commun en suivant mot à mot la définition 3.13.

Définition 3.14. *Soit* A *un anneau et soient* $d, x, y \in A$. *On appelle* plus grand diviseur commun de x, y (notation : $\mathrm{pgcd}(x, y)$) *tout* $d \in A$ *tel que*

- $d \mid x$ *et* $d \mid y$ *et*
- *pour tout* $e \in A$ *on a* $((e \mid x$ *et* $e \mid y) \Rightarrow e \mid d)$.

On définit également le plus petit multiple commun dans un anneau général en reprenant la définition dans $\mathbb{Z}$ (voir « structures mathématiques », en remplaçant $\mathbb{N}$ par $\mathbb{Z}$).

Définition 3.15. *Soient* $m \in A$ *et* $x, y \in A$. *On appelle* plus petit multiple commun de x, y (notation : $\mathrm{ppcm}(x, y)$) *tout* $m \in A$ *tel que*

- $x \mid m$ *et* $y \mid m$ *et*
- *pour tout* $n \in A$ *on a* $((x \mid n$ *et* $y \mid n) \Rightarrow m \mid n)$.

Attention ! Dans un anneau quelconque, ni pgcd ni ppcm n'existent en général ! Par contre pour $\mathbb{Z}$ nous avons démontré – à l'aide de l'algorithme d'Euclide, donc du fait que $\mathbb{Z}$ est un anneau euclidien – (voir « structures mathématiques ») que un/le pgcd (et aussi un/le ppcm) existe toujours et qu'il y a toujours une identité de Bézout. La même chose est vraie pour tous les anneaux euclidiens, comme on va le voir tout de suite.
D'abord encore une nouvelle définition pour bien exprimer la relation entre deux pgcd des mêmes nombres.

Définition 3.16. *Soit* A *un anneau intègre. On dit que* $a, b \in A$ *sont* associés *s'il existe* $u \in A^\times$ *(une unité) tel que* $a = ub$. *Notation :* $a \sim b$.

Exemple 3.17. *Comme les seules unités de* $\mathbb{Z}$ *sont* 1 *et* -1, *le seul élément de* $\mathbb{Z}$ *qui est associé à un élément* $n \in \mathbb{Z}$ *est* $-n$.

Lemme 3.18. *Être associés définit une relation d'équivalence sur l'anneau* A.

Démonstration. **Réflexivité** Soit $a \in A$. Alors $a \sim a$ car $a = 1 \cdot a$.

Symétrie Soient $a, b \in A$ tels que $a \sim b$. Il existe $u \in A^\times$ tel que $a = ub$. Donc $b = u^{-1}a$, donc $b \sim a$.

Transitivité Soient $a, b, c \in A$ tels que $a \sim b$ et $b \sim c$. Il existe $u, v \in A^\times$ tels que $a = ub$ et $b = vc$. Donc $a = uvc$ et $a \sim c$ car $uv \in A^\times$.

□

Proposition 3.19. *Soient A un anneau intègre et $a, b \in A$ deux éléments, pas tous les deux 0.*

(a) Si $a \mid b$ et $b \mid a$, alors $a \sim b$.

(b) Tous les pgcd de a et b sont associés. Plus précisement, si $d, e \in A$ sont tous les deux un plus grand diviseur commun de a et b, alors $d \sim e$. Nous écrivons $\mathrm{pgcd}(a, b) \sim d$.

(c) Tous les ppcm de a et b sont associés. Plus précisement, si $m, n \in A$ sont tous les deux un plus petit multiple commun de a et b, alors $m \sim n$. Nous écrivons $\mathrm{ppcm}(a, b) \sim n$.

Démonstration. (a) Il existe $r, s \in A$ tels que $a = rb$ et $b = sa$. Donc $a = rsa$ et $0 = a(1 - rs)$. En utilisant le fait que A est intègre, on conclut $1 - rs = 0$, donc $rs = 1$, donc $r, s \in A^\times$, donc $a \sim b$.
(b) et (c) sont une conséquence directe de (a) et de la deuxième partie de la définition du pgcd/ppcm.
□

Exemple 3.20. *(a) Soient $x, y \in \mathbb{Z}$ pas tous les deux 0. Puisque les unités de $\mathbb{Z}$ sont -1 et 1, le $\mathrm{pgcd}(x, y)$ et le $\mathrm{ppcm}(x, y)$ sont uniques à signe près. Par le $\mathrm{pgcd}(x, y)$* positif *et le $\mathrm{ppcm}(x, y)$* positif*, nous comprenons les uniques représentants positifs. C'est la notion « habituelle » du pgcd et du ppcm.*

(b) Soient $f, g \in K[X]$ pas tous les deux 0 où K est un corps. Puisque les unités de $K[X]$ sont $K^\times = K \setminus \{0\}$, le $\mathrm{pgcd}(f, g)$ et le $\mathrm{ppcm}(f, g)$ sont uniques à muliplication par une constante dans $K^\times$ près. Par le $\mathrm{pgcd}(f, g)$ unitaire *et le $\mathrm{ppcm}(f, g)$* unitaire*, nous comprenons les uniques représentants unitaires.*

Lemme 3.21. *Soient A un anneau et $x, y \in A$ pas tous les deux 0. Si $d \in A$ est un diviseur commun de x et y (c'est-à-dire, $d \mid x$ et $d \mid y$) et s'il existe $r, s \in A$ tels que $d = rx + sy$ (*relation de Bézout*), alors d est un $\mathrm{pgcd}(x, y)$.*

Démonstration. Soit $e \in A$ tel que $e \mid x$ et $e \mid y$. Il en suit que e divise $d = rx + sy$, montrant que d est un $\mathrm{pgcd}(x, y)$. □

Théorème 3.22 (Algorithme d'Euclide, identité de Bézout)**.** *Soit A un anneau euclidien (avec δ comme dans la définition 3.11). Alors, pour tout $a, b \in A$ qui ne sont pas 0 tous les deux, un plus grand commun diviseur $d \sim \mathrm{pgcd}(a, b)$ existe et il existe $r, s \in A$ tels que*

$$d = ra + sb.$$

Démonstration. On montre que l'algorithme d'Euclide donne le résultat.

- Préparation : On pose
$$\begin{cases} x_0 = a,\ x_1 = b & \text{si } \delta(a) \geq \delta(b), \\ x_0 = b,\ x_1 = a & \text{sinon.} \end{cases}$$
On pose aussi $B_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

- Si $x_1 = 0$, on **arrête** et on pose $d := x_0$.
  Si $x_1 \neq 0$, on fait la division euclidienne

$$x_0 = x_1 q_1 + x_2 \quad \text{où } q_1, x_2 \in A \text{ tels que } (x_2 = 0 \text{ ou } \delta(x_2) < \delta(x_1)).$$

  On pose $A_1 := \left(\begin{smallmatrix} -q_1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_1 := A_1 B_0$.
  On a $\left(\begin{smallmatrix} x_2 \\ x_1 \end{smallmatrix}\right) = A_1 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = B_1 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.

- Si $x_2 = 0$, on **arrête** et on pose $d := x_1$.
  Si $x_2 \neq 0$, on fait la division euclidienne

$$x_1 = x_2 q_2 + x_3 \quad \text{où } q_2, x_3 \in A \text{ tels que } (x_3 = 0 \text{ ou } \delta(x_3) < \delta(x_2)).$$

  On pose $A_2 := \left(\begin{smallmatrix} -q_2 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_2 := A_2 B_1$.
  On a $\left(\begin{smallmatrix} x_3 \\ x_2 \end{smallmatrix}\right) = A_2 \left(\begin{smallmatrix} x_2 \\ x_1 \end{smallmatrix}\right) = B_2 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.

- Si $x_3 = 0$, on **arrête** et on pose $d := x_2$.
  Si $x_3 \neq 0$, on fait la division euclidienne

$$x_2 = x_3 q_3 + x_4 \quad \text{où } q_3, x_4 \in A \text{ tels que } (x_4 = 0 \text{ ou } \delta(x_4) < \delta(x_3)).$$

  On pose $A_3 := \left(\begin{smallmatrix} -q_3 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_3 := A_3 B_2$.
  On a $\left(\begin{smallmatrix} x_4 \\ x_3 \end{smallmatrix}\right) = A_3 \left(\begin{smallmatrix} x_3 \\ x_2 \end{smallmatrix}\right) = B_3 \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.

- $\cdots$

- Si $x_n = 0$, on **arrête** et on pose $d := x_{n-1}$.
  Si $x_n \neq 0$, on fait la division euclidienne

$$x_{n-1} = x_n q_n + x_{n+1} \quad \text{où } q_n, x_{n+1} \in A \text{ tels que } (x_{n+1} = 0 \text{ ou } \delta(x_{n+1}) < \delta(x_n)).$$

  On pose $A_n := \left(\begin{smallmatrix} -q_n & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $B_n := A_n B_{n-1}$.
  On a $\left(\begin{smallmatrix} x_{n+1} \\ x_n \end{smallmatrix}\right) = A_n \left(\begin{smallmatrix} x_n \\ x_{n-1} \end{smallmatrix}\right) = B_n \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right)$.

- $\cdots$

Il est clair que l'algorithme ci-dessus (c'est l'algorithme d'Euclide !) s'arrête car

$$\delta(x_n) < \delta(x_{n-1}) < \cdots < \delta(x_2) < \delta(x_1)$$

sont des nombres naturels.
Supposons que l'algorithme se termine avec $x_n = 0$. Donc, $d = x_{n-1}$. Nous avons par construction :

$$\left(\begin{smallmatrix} x_n \\ x_{n-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right) = B_{n-1} \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & \beta \\ r & s \end{smallmatrix}\right) \left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha x_1 + \beta x_0 \\ r x_1 + s x_0 \end{smallmatrix}\right),$$

montrant

$$d = r x_1 + s x_0.$$

Noter que le déterminant de A_i est -1 pour tout i, donc $\det(B_{n-1}) = (-1)^{n-1}$. Alors $C := (-1)^{n-1}\left(\begin{smallmatrix} s & -\beta \\ -r & \alpha \end{smallmatrix}\right)$ est l'inverse de B_{n-1}. Donc

$$\left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = CB_{n-1}\left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = C\left(\begin{smallmatrix} 0 \\ d \end{smallmatrix}\right) = \left(\begin{smallmatrix} d(-1)^n\beta \\ d(-1)^{n-1}\alpha \end{smallmatrix}\right),$$

montrant $d \mid x_1$ et $d \mid x_0$. Le lemme 3.21 implique donc que d est un pgcd de x_0 et x_1. □

Corollaire 3.23. *Soient A un anneau euclidien et $a, b, d, y \in A$ avec $a \neq 0$ ou $b \neq 0$.*

(a) Si $d \sim \operatorname{pgcd}(a, b)$, alors $1 \sim \operatorname{pgcd}(\frac{a}{d}, \frac{b}{d})$.

(b) Si $1 \sim \operatorname{pgcd}(a, b)$ et $a \mid y$ et $b \mid y$, alors $ab \mid y$.

(c) Un $\operatorname{ppcm}(a, b)$ existe et on a

$$\operatorname{ppcm}(a, b) \sim \frac{ab}{d} \text{ où } d \sim \operatorname{pgcd}(a, b).$$

Démonstration. (a) L'identité de Bézout divisée par d nous donne la relation

$$1 = r\frac{a}{d} + s\frac{b}{d}.$$

Par le lemme 3.21, 1 est un plus grand commun diviseur de $\frac{a}{d}$ et $\frac{b}{d}$.
(b) On part de l'identité de Bézout

$$1 = ra + sb.$$

Comme $a \mid y$, il existe $u \in A$ tel que $y = ua$. Multiplier la dernière égalité par r donne

$$ry = ura = u(1 - sb) = u - sbu,$$

donc

$$u = ry + sbu.$$

Comme $b \mid y$, on obtient $b \mid u$, donc il existe $v \in A$ tel que $u = vb$. Alors, nous avons $y = ua = v(ab)$.
(c) Soit $x := \frac{ab}{d}$. Il suffit de vérifier la définition :

- $x = a\frac{b}{d}$, donc $a \mid x$.
- $x = b\frac{a}{d}$, donc $b \mid x$.
- Soit $y \in A$ tel que $a \mid y$ et $b \mid y$. Alors $\frac{a}{d} \mid \frac{y}{d}$ et $\frac{b}{d} \mid \frac{y}{d}$. Par (a) nous avons $1 \sim \operatorname{pgcd}(\frac{a}{d}, \frac{b}{d})$. Utilisant (b) on en conclut $\frac{ab}{dd} \mid \frac{y}{d}$, donc $x = \frac{ab}{d} \mid y$.

□

4 Anneaux intègres

Objectifs :

- Maîtriser les corps des fractions d'anneau intègre et savoir les expliquer en tant que généralisations des nombres rationnels ;
- connaître les notions d'élément irréductible et d'élément premier, et les relations entre elles ; savoir expliquer la signification de ses notions pour les entiers relatifs et les polynômes à coefficients dans un corps ;
- connaître la notion d'idéal engendré par des générateurs ;
- connaître et savoir appliquer la définition et les résultats principaux concernant les anneaux principaux ;
- savoir démontrer que tout anneau euclidien est principal ;
- connaître la définition d'idéal maximal et premier, ainsi que leur caractérisation en termes d'anneau intègre et corps ;
- connaître des exemples et savoir démontrer des propriétés simples.

Corps des fractions

Nous commençons par la définition du corps des fractions d'un anneau intègre qui généralise de façon directe la construction des nombres rationnels.
Nous expliquons l'idée dans $\mathbb{Z}$. Deux fractions $\frac{a}{x}$ et $\frac{b}{y}$ (avec a, b, x, y dans $\mathbb{Z}$ et $x \neq 0 \neq y$) représentent le même nombre rationnel si et seulement si $\frac{ay}{xy}$ et $\frac{bx}{xy}$ représentent le même nombre rationnel. Cela est le cas si et seulement si $ay = bx$. L'idée principale est de regarder une fraction $\frac{a}{x}$ comme une classe d'équivalence pour la relation d'équivalence décrite et formalisée dans la définition suivante.

Définition-Lemme 4.1. *Soit A un anneau intègre. Sur $A \times (A \setminus \{0\})$ on définit une relation binaire par*

$$(a, x) \sim (b, y) \Leftrightarrow ay = bx.$$

C'est une relation d'équivalence.
La classe de (a, x) est formée de tous les (b, y) tel que $ay = bx$.
Nous utilisons la notation $\frac{a}{x}$ pour la classe d'équivalence de (a, x).
L'ensemble quotient est noté $\mathrm{Frac}(A)$.

Démonstration. Exercice. □

Proposition 4.2. *Soit $K := \mathrm{Frac}(A)$ l'ensemble quotient de la définition-lemme 4.1.*

(a) Les deux applications

$$+ : K \times K \to K, \quad \frac{a}{x} + \frac{b}{y} := \frac{ay + bx}{xy}$$

et

$$\cdot : K \times K \to K, \quad \frac{a}{x} \cdot \frac{b}{y} := \frac{ab}{xy}$$

sont bien définies, c'est-à-dire que leurs définitions ne dépendent pas des choix des représentants (a, x) *et* (b, y) *des classes* $\frac{a}{x}$ *et* $\frac{b}{y}$.

(b) $(K, +, \cdot, \frac{0}{1}, \frac{1}{1})$ *est un corps (commutatif!) appelé* corps des fractions de A.

(c) L'application

$$\iota : A \to K, \quad a \mapsto \frac{a}{1}$$

est un homomorphisme injectif d'anneaux.

Démonstration. Exercice. □

Exemple 4.3. *(a) Le corps des fractions de* $\mathbb{Z}$ *est* $\mathbb{Q}$ *(par définition!).*

(b) Soit K *un corps. Nous notons* $K(X)$ *le corps des fractions de l'anneau des polynômes* $K[X]$. *Ses éléments sont donc des classes d'équivalences* $\frac{f}{g}$ *avec* $f, g \in K[X]$ *et* $g \neq 0$ *(on insiste que* $g \neq 0$ *signifie que* g *n'est pas égal au polynôme constant* 0 *et pas que* g *ne possède aucune racine ; g peut avoir des racines).*

Définitions générales

Au lycée, on définit un nombre premier comme un $p \in \mathbb{Z}_{\geq 2}$ dont les seuls diviseurs positifs sont 1 et p. Cela est équivalent à ce que p ne s'écrive pas comme produit $p = ab$ sauf si $a \in \{1, -1\} = \mathbb{Z}^\times$ ou $b \in \{1, -1\} = \mathbb{Z}^\times$. On pourrait alors dire (et on le dira aussi – voir la prochaine définition) que p est irréductible dans le sens qu'il ne se factorise pas de façon non triviale.
On peut aussi donner la caractérisation suivante qu'un $p \in \mathbb{Z}_{\geq 2}$ est un nombre premier (voir appendice de « structures mathématiques ») :

p est premier $\Leftrightarrow$ si p divise un produit ab avec $a, b \in \mathbb{Z}$, alors $p \mid a$ ou $p \mid b$.

Nous allons utiliser cette caractérisation comme notre définition d'élément premier dans un anneau intègre quelconque.

Définition 4.4. *Soit* A *un anneau intègre et* $0 \neq p \in A \setminus A^\times$.

(a) p *est dit* irréductible *si l'assertion suivante est vraie :*

Pour tout $a, b \in A$ *: si* $p = ab$, *alors* $a \in A^\times$ *ou* $b \in A^\times$.

(b) p *est dit* (élément) premier *si l'assertion suivante est vraie :*

Pour tout $a, b \in A$ *: si* $p \mid ab$, *alors* $p \mid a$ *ou* $p \mid b$.

Remarque 4.5. *(a)* ***Par définition*** *une unité (c'est-à-dire un élément de* $A^\times$*) n'est ni premier ni irréductible. Ainsi, par exemple,* 1 *et* -1 *ne sont jamais ni premier ni irréductible.*

(b) On définit ci-dessus deux notions à priori différentes : élément premier et élément irréductible. Dans certains anneaux (voir plus bas), ces deux notions sont les mêmes, mais ***pas toujours****.*

Exemple 4.6. *(a) Soit $u \in A^\times$ une unité. Si $0 \neq p \in A \setminus A^\times$ est premier, alors up est aussi premier. Si $0 \neq p \in A \setminus A^\times$ est irréductible, alors up est aussi irréductible.*

(b) Pour $n \in \mathbb{Z}_{\geq 2}$ on a l'équivalence

$$n \text{ est premier } \Leftrightarrow n \text{ est irréductible.}$$

Nous allons démontrer cette équivalence dans le contexte des anneaux euclidiens tout de suite.

Pour $A = \mathbb{Z}$ et $0 \neq n \in \mathbb{Z} \setminus \{-1, 1\} = \mathbb{Z} \setminus \mathbb{Z}^\times$, on a que n est premier si et seulement si $|n|$ est un nombre premier. Autrement dit, si $n \in \mathbb{Z}_{\geq 2}$ est un nombre premier, alors n et $-n$ sont des éléments premiers de l'anneau $\mathbb{Z}$.

(c) Soit $A = K[X]$ pour un corps K. Les polynômes de degré 1 sont irréductibles. Car, si $f = gh$ pour $f, g, h \in K[X]$ on a $1 = \deg(f) = \deg(g) + \deg(h)$ et donc $\deg(g) = 0$ ou $\deg(h) = 0$, d'où g ou h est constant et donc une unité.

D'abord un petit lemme.

Lemme 4.7. *Soit A un anneau intègre et $0 \neq p \in A \setminus A^\times$ premier. Si p divise un produit $a_1 a_2 \cdots a_n$ (avec $a_1, \ldots, a_n \in A$ et $n \in \mathbb{N}$), alors il existe $i \in \{1, \ldots, n\}$ tel que $p \mid a_i$.*

Démonstration. C'est une récurrence simple. Pour $n = 1$, l'assertion est triviale. Pour $n = 2$ c'est précisement la définition. Supposons le résultat démontré pour $n - 1 \geq 1$. Du fait que p divise $(a_1 \ldots a_{n-1}) \cdot a_n$ on conclut par la définition $p \mid a_1 \ldots a_{n-1}$ ou $p \mid a_n$. Dans le dernier cas nous avons terminé ($i = n$) ; dans le premier cas, par l'hypothèse de récurrence il existe $i \in \{1, \ldots, n-1\}$ tel que $p \mid a_i$ et nous avons aussi terminé. □

Dans l'exemple de $\mathbb{Z}$ nous savons que les éléments premiers et les éléments irréductibles sont les mêmes. En général cela n'est pas vrai, mais nous avons toujours l'implication que tout élément premier est irréductible :

Proposition 4.8. *Soit A un anneau intègre et $0 \neq p \in A \setminus A^\times$ premier. Alors p est irréductible.*

Démonstration. Soient $a, b \in A$ tels que $p = ab$. Cela implique que p divise ab. Comme p est premier, par définition $p \mid a$ ou $p \mid b$. Quitte à échanger a et b, sans perte de généralité nous supposons $p \mid a$. Donc il existe $c \in A$ tel que $a = pc$. Nous obtenons $p = ab = pbc$, alors $0 = p(1 - bc)$. Comme A est intègre, on a $1 = bc$, alors $b \in A^\times$. Nous avons donc vérifié que p est irréductible. □

Anneaux principaux

Définition 4.9. *Soit A un anneau.*

(a) Soient $a_1, \ldots, a_n \in A$. On note $(a_1, \ldots, a_n)$ l'idéal engendré par $a_1, \ldots, a_n$ *:*

$$(a_1, \ldots, a_n) := Aa_1 + \cdots + Aa_n := \left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, \ldots, r_n \in A \right\}.$$

(b) Un idéal $I \trianglelefteq A$ est dit principal *s'il existe $a \in A$ tel que $I = (a)$.*

Exemple 4.10. *(a) Soit $n \in \mathbb{Z}$. Alors $n\mathbb{Z} = (n) = \{nm \mid m \in \mathbb{Z}\}$ est un idéal principal de $\mathbb{Z}$.*

(b) Dans $\mathbb{Z}$ nous avons l'égalité $(2, 3) = (1) = \mathbb{Z}$.

Raison : « $\subseteq$ » est clair. « $\supseteq$ » : $1 = 3 - 2 \in (2, 3)$.

(c) $(2, X) \trianglelefteq \mathbb{Z}[X]$ n'est pas un idéal principal (exercice).

Lemme 4.11. *Soient A un anneau et $a, b \in A$.*

(a) $(a) \subseteq (b) \Leftrightarrow b \mid a$

(b) $(a) = (b) \Leftrightarrow a$ et b sont associés

Démonstration. (a) Si $(a) \subseteq (b)$, alors il existe $c \in A$ tel que $a = cb$, alors $b \mid a$. Si $b \mid a$, alors il existe $c \in A$ tel que $a = cb$, alors $(a) \subseteq (b)$.
(b) Par (a), $(a) = (b)$ équivaut à ($a \mid b$ et $b \mid a$). Donc $a \sim b$. Si $a \sim b$, alors il existe une unité $u \in A^\times$ tel que $a = ub$, alors $(a) = (ub) = (b)$. □

Définition 4.12. *On appelle* anneau principal *tout anneau commutatif et intègre A tel que tout idéal de A est principal.*

Théorème 4.13. *Tout anneau euclidien est principal.*

Démonstration. Soient A un anneau euclidien (pour δ) et $I \trianglelefteq A$ un idéal. Nous allons montrer que I est un idéal principal. Si $I = \{0\}$, on a $I = (0)$, et I est principal (0 est le générateur).
Supposons donc $I \neq (0)$. Alors, l'ensemble

$$\{\delta(i) \mid i \in I, i \neq 0\} \subseteq \mathbb{N}$$

est non vide et possède donc un plus petit élément $\delta(a)$ pour un $0 \neq a \in I$. Comme $a \in I$, on a l'inclusion $(a) \subseteq I$. Nous allons démontrer l'autre.
Soit $x \in I$. La division euclidienne donne

$$x = qa + r \text{ où } q, r \in A \text{ tels que } \big(r = 0 \text{ ou } \delta(r) < \delta(a)\big).$$

Mais, $r \in I$ car $r = x - qa \in I$. Alors, soit $r = 0$, soit $\delta(r) \geq \delta(a)$. Comme la dernière possibilité est exclue, on a $r = 0$, donc $x = qa \in (a)$. Cela montre $I \subseteq (a)$, donc $I = (a)$ est un idéal principal. □

Exemple 4.14. *(a) $\mathbb{Z}$ est un anneau principal.*

(b) $K[X]$ est un anneau principal si K est un corps.

(c) Tout corps est un anneau principal. En fait, tout idéal $\{0\} \neq I \lhd K$ est égal à $(1) = K$.

Raison : Soit $0 \neq i \in I$. Comme K est un corps, i possède un inverse i^{-1}. Donc $1 = i^{-1}i \in I$, alors $(1) \subseteq I$, donc $(1) = I$.

(d) $\mathbb{Z}[X]$ n'est pas un anneau principal car par exemple $(2, X)$ n'est pas un idéal principal (exercice).

(e) L'anneaux $K[X,Y]$ des polynômes dans les variables X, Y et à coefficients dans K n'est pas principal car (X,Y) n'est pas un idéal principal.

Nous voyons maintenant que dans un anneau principal le pgcd et le ppcm existent toujours.

Proposition 4.15. *Soient A un anneau principal et $a, b, d, m \in A$ avec $a \neq 0$ ou $b \neq 0$.*

(a) $d \sim \mathrm{pgcd}(a,b) \Leftrightarrow (d) = (a,b)$.

(b) $m \sim \mathrm{ppcm}(a,b) \Leftrightarrow (m) = (a) \cap (b)$.

Démonstration. (a) « $\Leftarrow$ » : Comme $a, b \in (d)$ on a $d \mid a$ et $d \mid b$. Cela montre que d est un diviseur commun de a et b. Comme $(d) = (a,b)$ il existe $r, s \in A$ tels que $d = ra + sb$. Le lemme 3.21 implique que d est un $\mathrm{pgcd}(a,b)$.
« $\Rightarrow$ » : Soit $e \in A$ tel que $(e) = (a,b)$. L'implication « $\Leftarrow$ » montre que e est un $\mathrm{pgcd}(a,b)$. Nous savons que si d est un $\mathrm{pgcd}(a,b)$, alors $d \sim e$. Cela montre $(e) = (d) = (a,b)$.
(b) La vérification pour le ppcm est très similaire à celle pour le pgcd. □

Dans un anneau principal nous avons l'équivalence de « premier » et « irréductible » :

Proposition 4.16. *Soit A un anneau principal et $0 \neq p \in A \setminus A^\times$. Alors*

$$p \text{ est premier } \Leftrightarrow p \text{ est irréductible.}$$

Démonstration. « $\Rightarrow$ » : Proposition 4.8.
« $\Leftarrow$ » : Soient $a, b \in A$ tel que $p \mid ab$. Il existe $c \in A$ tel que $ab = pc$. Supposons que p ne divise pas a (sinon, nous avons déjà terminé). Il existe $m \in A$ tel que

$$(p) \subsetneq (p,a) = (m),$$

où nous avons utilisé le fait que A est principal en écrivant l'idéal (p,a) comme idéal principal. Donc $p \in (m)$ et alors $m \mid p$: il existe $n \in A$ tel que $p = mn$. Maintenant nous utilisons que p est irréductible : $m \in A^\times$ ou $n \in A^\times$. Si $n \in A^\times$, alors $(p) = (m)$ ce qui est exclu. Donc $m \in A^\times$. Alors $1 = m^{-1}m \in (m) = (p,a)$. Il existe donc $r, s \in A$ tels que $1 = rp + sa$. On multiplie cette égalité par b pour obtenir $b = prb + abs = prb + pcs = p(rb + cs)$. Donc $p \mid b$, comme il fallait montrer pour conclure que p est premier. □

Idéaux premiers et maximaux

Définition 4.17. *Soit A un anneau.*

(a) On appelle premier *tout idéal $I \lhd A$ tel que $I \neq A$ et l'assertion suivante est vraie :*

$$\forall\, a, b \in A : \textit{si } a \cdot b \in I \textit{ avec } a, b \in A, \textit{ alors } a \in I \textit{ ou } b \in I.$$

(b) On appelle maximal *tout idéal $I \lhd A$ tel que $I \neq A$ et il n'existe aucun idéal J satisfaisant $I \subsetneq J \subsetneq A$.*

Lemme 4.18. *Soit A un anneau. Alors les assertions suivantes sont vraies.*

(a) A *est intègre* $\Leftrightarrow (0)$ *est un idéal premier.*

(b) A *est un corps* $\Leftrightarrow (0)$ *est un idéal maximal.*

Démonstration. (a) « $\Rightarrow$ » : Supposons que A est intègre et soient $a, b \in A$ tels que $ab \in (0)$, donc $ab = 0$, donc $a = 0$ ou $b = 0$ par l'intégrité, donc $a \in (0)$ ou $b \in (0)$. Nous avons montré que (0) est un idéal premier.
« $\Leftarrow$ » : Supposons maintenant que (0) est un idéal premier. Soient $a, b \in A$ tels que $ab = 0$. Donc $ab \in (0)$, alors $a \in (0)$ ou $b \in (0)$ par la primalité, donc $a = 0$ ou $b = 0$. Nous avons montré que A est intègre.
(b) « $\Rightarrow$ » : Supposons que A est un corps et soit $0 \subsetneq I \subseteq A$ un idéal. Puisque I contient un élément non-nul $x \in I$, il contient aussi tous ces multiples, en particulier $(ax^{-1})x = a$ pour tout $a \in A$, donc $I = A$.
« $\Leftarrow$ » : Soit $0 \neq a \in A$. Puisque $(0) \neq (a)$, la maximalité de (0) implique $(a) = A$. Donc il existe $b \in A$ tel que $1 = ab$. Cela montre que a est inversible. □

La définition est motivée par l'interprétation suivante :

Proposition 4.19. *Soient* A *un anneau intègre et* $0 \neq p \in A \setminus A^\times$.

(a) $(p) \lhd A$ *est (un idéal) premier* $\Leftrightarrow p$ *est (un élément) premier.*

(b) $(p) \lhd A$ *est (un idéal) maximal* $\Rightarrow p$ *est (un élément) irréductible.*

Démonstration. (a) Il suffit de se rappeler : $p \mid ab \;\Leftrightarrow\; ab \in (p)$.
(b) Soit $p = ab$ avec $a, b \in A$. Donc $a \mid p$, donc $(p) \subseteq (a) \trianglelefteq A$. La maximalité de (p) implique : soit $(p) = (a)$ (dans ce cas $b \in A^\times$), soit $(a) = A$ (dans ce cas $a \in A^\times$). Alors p est irréductible. □

L'implication inverse de (b) n'est pas vraie en général, mais elle est valable dans les anneaux principaux :

Proposition 4.20. *Soient* A *un anneau principal et* $0 \neq p \in A \setminus A^\times$. *Alors :*
$(p) \lhd A$ *est (un idéal) maximal* $\Leftrightarrow p$ *est (un élément) irréductible.*

Démonstration. Par (b) de la proposition 4.19 il suffit de démontrer « $\Leftarrow$ ». Soit p donc irréductible et soit $J \lhd A$ un idéal tel que $(p) \subseteq J$ et $J \neq A$. Comme l'anneau est principal, on a $J = (j)$ pour un $j \in J$. Comme J n'est pas A, l'élément j n'est pas inversible dans A. L'inclusion $(p) \subseteq (j)$ implique $j \mid p$, donc $p = jb$ pour un $b \in A$. Comme p est irréductible, alors $b \in A^\times$ et alors $(p) = (j) = J$, montrant que (p) est un idéal maximal. □

Par ce que l'on a vu, la théorie des idéaux premiers et maximaux dans un anneau principal est très simple :

Proposition 4.21. *Soit* A *un anneau principal.*

(a) Les idéaux premiers de A *sont* (0) *et les idéaux principaux engendrés par les éléments premiers.*

(b) On suppose ici que (0) n'est pas un idéal maximal dans A (donc que A n'est pas un corps par le lemme 4.18). Les idéaux maximaux de A sont les idéaux principaux engendrés par les éléments premiers.

Démonstration. Tout idéal est principal par définition, donc de la forme (a). L'idéal (0) est premier car l'anneau est intègre. Pour toute unité $a \in A^\times$, l'idéal $(a) = A$, donc il n'est ni premier ni maximal. Soit $0 \neq a \in A \setminus A^\times$. Les propositions 4.16, 4.19(a) et 4.20 nous assurent des équivalences :

$$(a) \text{ premier } \Leftrightarrow a \text{ premier } \Leftrightarrow a \text{ irréductible } \Leftrightarrow (a) \text{ maximal.}$$

Cela achève la preuve. □

Proposition 4.22. *Soient A un anneau et $I \lhd A$, $I \neq A$ un idéal.*

(a) I est premier $\Leftrightarrow$ A/I est intègre.

(b) I est maximal $\Leftrightarrow$ A/I est un corps.

(c) I est maximal $\Rightarrow$ I est premier.

Démonstration. (a) « $\Rightarrow$ » : Supposons $(a+I)(b+I) = 0+I$. Alors $ab+I = 0+I$, donc $ab \in I$. Comme I est premier, $a \in I$ ou $b \in I$. En conséquence, $a+I = 0+I$ ou $b+I = 0+I$. Nous avons montré que le seul diviseur de zéro dans A/I est $0+I$, alors, A/I est intègre.
« $\Leftarrow$ » : Supposons que $ab \in I$. Alors $0+I = ab+I = (a+I)(b+I)$. Comme A/I est intègre, on a $a+I = 0+I$ ou $b+I = 0+I$, donc $a \in I$ ou $b \in I$. Cela montre que I est un idéal premier.
(b) « $\Rightarrow$ » : Soit $a+I \neq 0+I$. On doit montrer que $a+I$ est inversible. Comme $a+I \neq 0+I$, on a $a \notin I$. Soit $J = (I, a)$, l'idéal engendré par a et I. Donc $I \subsetneq (I, a)$. La maximalité de I implique $J = A$. Donc $1 \in J$, donc $1 = i + ra$ pour un $i \in I$ et un $r \in A$. En conséquence $1 + I = ra + I = (a+I)(r+I)$, et nous avons trouvé l'inverse.
« $\Leftarrow$ » : On veut montrer que I est maximal. Soit donc $J \trianglelefteq A$ un idéal tel que $I \subsetneq J$. Soit $a \in J \setminus I$. Comme $a \notin I$, l'élément $a+I$ de A/I possède un inverse $1+I = (a+I)(b+I)$. La relation $1 \in ab + I \subseteq J$ montre $J = A$ et donc la maximalité de I.
(c) I maximal $\Rightarrow$ A/I corps $\Rightarrow$ A/I anneau intègre $\Rightarrow$ I est premier. □

Exemple 4.23. *(a) Soit $p \in \mathbb{Z}$ un nombre premier. Alors, le quotient $\mathbb{F}_p := \mathbb{Z}/(p)$ est un corps fini.*

(b) Soit K un corps et soit $f \in K[X]$ un polynôme irréductible. Alors, le quotient $K[X]/(f(X))$ est un corps.

Existence d'idéaux maximaux

En « structures mathématiques » nous avons introduit les ensembles d'un point de vue intuitif et non rigoureux. Un traitement strict ne peut se faire que dans un cours de logique à un moment plus avancé (un tel cours n'est pas offert à l'UL en ce moment – vous pouvez regarder des livres pour plus de détails). Dans la théorie des ensembles il y a un axiome important : « l'axiome du choix ».[1] Dans la

[1] L'axiome du choix : Soit X un ensemble dont les éléments sont des ensembles non vides. Alors il existe une fonction f définie sur X qui à chaque $M \in X$ associe un élément de M. Une telle fonction est appelée « fonction du choix ».

théorie des ensembles on montre le « lemme de Zorn » qui dit que l'axiome du choix est équivalent à l'assertion suivante.

Axiome 4.24 (Lemme de Zorn)**.** *Soit S un ensemble non-vide et $\leq$ une relation d'ordre sur S.*[2] *On fait l'hypothèse suivante : Tout sous-ensemble $T \subseteq S$ qui est totalement ordonné*[3] *possède un majorant.*[4] *Alors, S contient un élément maximal.*[5]

Le lemme de Zorn peut être utilisé pour démontrer que tout espace vectoriel possède une base (voir le cours « algèbre linéaire 2 »). Nous l'appliquons ici pour obtenir l'existence d'idéaux maximaux.

Proposition 4.25. *Soit $A \neq \{0\}$ un anneau. Alors A possède un idéal maximal.*

Démonstration. On utilise le lemme de Zorn 4.24. Soit

$$S := \{I \lhd A \text{ idéal} \mid I \neq A\}.$$

L'ensemble S est non-vide car $(0) \in S$. L'inclusion d'ensembles « $\subseteq$ » définit une relation d'ordre sur S.
On vérifie que l'hypothèse du lemme de Zorn est satisfaite : Soit $T \subseteq S$ un sous-ensemble totalement ordonné. On doit produire un majorant $E \in S$ pour T. On pose $E = \bigcup_{I \in T} I$. Il faut démontrer que E est un idéal de A différent de A. Soient $x, y \in E$ et $a \in A$. Il existe $I_x, I_y \in T$ tels que $x \in I_x$ et $y \in I_y$. Comme T est totalement ordonné, on sait $I_x \subseteq I_y$ ou $I_y \subseteq I_x$. Soit $I = I_x \cup I_y$, alors $I = I_x$ ou $I = I_y$. Alors $x, y \in I$. Comme c'est un idéal, on a $x - y \in I \subseteq E$ et $ax \in I \subseteq E$. Cela montre que E est un idéal. Pour montrer $E \neq A$ on suppose le contraire. Dans ce cas $1 \in E$. Alors il existe $I \in T$ tel que $1 \in I$. Mais cela implique $I = A$, une contradiction. Donc E est bien un majorant pour T.
Le lemme de Zorn nous produit un élément maximal $\mathfrak{m} \in S$. Par définition c'est un idéal maximal. □

Corollaire 4.26. *Soit $A \neq \{0\}$ un anneau.*

(a) Tout idéal $I \lhd A$, $I \neq A$ est contenu dans un idéal maximal.

(b) Tout $x \in A \setminus A^\times$ est contenu dans un idéal maximal.

Démonstration. (a) Soit $\pi : A \twoheadrightarrow A/I$ la projection naturelle qui envoie a sur $a + I$. Par la proposition 4.25 il existe un idéal maximal $\mathfrak{m} \subseteq A/I$. Soit $M := \pi^{-1}(\mathfrak{m})$ l'image réciproque de $\mathfrak{m}$ par π. Autrement dit, M est le noyau de l'homomorphisme d'anneaux composé $\varphi : A \xrightarrow{\pi} A/I \xrightarrow{\text{proj. naturelle}} (A/I)/\mathfrak{m}$. Comme cet homomorphisme est surjectif, le théorème d'isomorphisme donne l'isomorphisme d'anneaux $\overline{\varphi} : A/M \to (A/I)/\mathfrak{m}$. Puisque $\mathfrak{m}$ est maximal, par la proposition 4.22 $(A/I)/\mathfrak{m}$ est un corps, donc A/M est un corps, donc M est maximal.
(b) Utiliser (a) avec $I = (x)$. □

[2] On rappelle que par définition les trois points suivants sont satisfaits :

- $s \leq s$ pour tout $s \in S$.
- Si $s \leq t$ et $t \leq s$ pour $s, t \in S$, alors $s = t$.
- Si $s \leq t$ et $t \leq u$ pour $s, t, u \in S$, alors $s \leq u$.

[3] T est totalement ordonné si T est ordonné et pour tout couple $s, t \in T$ on a $s \leq t$ ou $t \leq s$.
[4] $g \in S$ est un majorant pour T si $t \leq g$ pour tout $t \in T$.
[5] $m \in S$ est maximal si pour tout $s \in S$ tel que $m \leq s$ on a $m = s$.

5 Anneaux factoriels

Objectifs :

- Maîtriser la notion d'anneau factoriel et ses propriétés principales ;
- connaître des systèmes de représentants des éléments irréductibles à association près et son lien aux nombres premiers « habituels » ;
- connaître et savoir appliquer les valuation et l'expression des pgcd et ppcm en termes de valuations ;
- connaître des exemples et savoir démontrer des propriétés simples.

Un des théorèmes principaux sur les entiers relatifs est le « théorème principal de la théorie élémentaire des nombres » : Tout entier $0 \neq n \in \mathbb{Z}$ s'écrit de façon unique (à numérotation près) comme produit fini de nombres premiers.
Nous allons retrouver ce théorème ici dans la formulation « $\mathbb{Z}$ est un anneau factoriel » qui sera une conséquence de : « tout anneau principal est un anneau factoriel ». Pour obtenir ce résultat il nous faut quelques préparations. D'abord la définition.

Définition 5.1. *On appelle* anneau factoriel *tout anneau intègre A tel que tout $0 \neq a \in A \setminus A^\times$ s'écrit comme produit fini d'éléments premiers, c'est-à-dire qu'il existe $n \in \mathbb{N}$ et $p_1, \dots, p_n \in A \setminus A^\times$ premiers tels que $a = p_1 \cdot p_2 \cdots p_n$.*

Proposition 5.2. *Soit A un anneau factoriel et $0 \neq p \in A \setminus A^\times$. Alors*

$$p \text{ est premier } \Leftrightarrow p \text{ est irréductible.}$$

Démonstration. « $\Rightarrow$ » : Proposition 4.8.
« $\Leftarrow$ » : Par la définition des anneaux factoriels, il existe $n \in \mathbb{N}$ et $p_1, \dots, p_n \in A \setminus A^\times$ premiers tels que $p = p_1 \cdot p_2 \cdots p_n$. Le fait que p est irréductible implique $n = 1$ et $p = p_1$, donc p est premier. □

Pour la suite nous avons besoin d'un ensemble $\mathbb{P}$ de représentants des éléments irréductibles à association près. Nous l'illustrons pour $A = \mathbb{Z}$ et $A = K[X]$ (avec K un corps).

Lemme 5.3. *(a) Soit $\mathbb{P} \subset \mathbb{Z}$ l'ensemble des nombres premiers positifs (habituels). Alors, $\mathbb{P}$ est un ensemble de représentants des éléments irréductibles dans $\mathbb{Z}$ à association près, c'est-à-dire, pout tout $n \in \mathbb{Z} \setminus \{-1, 0, +1\}$ irréductible on a soit $n \in \mathbb{P}$, soit $-n \in \mathbb{P}$, et pour tout $n, m \in \mathbb{P}$ avec $n \neq m$ on a $n \not\sim m$.*

(b) Soit K un corps et $\mathbb{P}$ l'ensemble des polynômes unitaires et irréductibles dans $K[X]$. Alors, $\mathbb{P}$ est un ensemble de représentants des éléments irréductibles dans $K[X]$ à association près, c'est-à-dire, pour tout irréductible $f \in K[X] \setminus (K^\times \cup \{0\})$ il existe une unique unité $a \in K^\times$ telle que $af \in \mathbb{P}$ (noter que a est l'inverse du coefficient dominant de f), et pour tout $f, g \in \mathbb{P}$ avec $f \neq g$ on a $f \not\sim g$.

Démonstration. (a) Voici les faits que nous utilisons :

- $\mathbb{Z}$ est euclidien.
- $\mathbb{Z}^\times = \{-1, +1\}$.
- $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$ est un élément premier si et seulement si n est irréductible.

Soit $n \in \mathbb{Z} \setminus \{-1, 0, +1\}$ irréductible, donc premier. Si $n > 0$, alors $n \in \mathbb{P}$. Si $n < 0$, alors $-n \in \mathbb{P}$. Il est clair que $n \in \mathbb{P}$ et $-n \in \mathbb{P}$ s'excluent (c'est l'unicité). Si n, m sont deux nombres premiers positifs distincts, il est clair que n n'est pas $-m$.
(b) Ici nous avons les faits établis en haut :

- $K[X]$ est euclidien.
- $K[X]^\times = K^\times$.

Soient $f \in K[X] \setminus (K^\times \cup \{0\})$ irréductible et b son coefficient dominant (toujours non-nul, donc une unité dans le corps K). Avec $a = b^{-1}$ nous avons que af est unitaire, donc $af \in \mathbb{P}$. Pour obtenir l'unicité, supposons $af = a'f \in \mathbb{P}$ ce qui implique bien $a = a'$. Soient $f, g \in \mathbb{P}$. Supposons $f \sim g$, donc $f = ag$ pour un $a \in K^\times$. Comme f et g sont tous les deux unitaires, il suffit de regarder le monôme dominant pour voir $a = 1$, donc $f = g$. □

Proposition 5.4. *Soit A un anneau intègre. Soit $\mathbb{P}$ un ensemble de représentants des éléments irréductibles de A à association près. Les assertions suivantes sont équivalentes :*

(i) A est factoriel.

(ii) Pour tout $0 \neq a \in A$ il existe une unique unité $u \in A^\times$, un unique $n \in \mathbb{N}_{\geq 0}$ et des uniques $p_1, \ldots, p_n \in \mathbb{P}$ (à l'ordre près) tels que

$$a = u \cdot p_1 \cdot p_2 \cdots p_n.$$

Démonstration. « (i) ⇒ (ii) » : Pour cette partie nous utiliserons qu'un élément est irréductible si et seulement s'il est premier (proposition 5.2).
Existence : Soit $0 \neq a \in A$. Comme on suppose donc que A est factoriel, il existe $n \in \mathbb{N}_{\geq 0}$ et des éléments premiers $p'_1, \ldots, p'_n$ tels que $a = p'_1 \cdot p'_2 \cdots p'_n$. Comme tout élément premier est irréductible (proposition 4.8) et $\mathbb{P}$ est un ensemble de représentants des éléments irréductibles à association près, il existe $u_1, \ldots, u_n \in A^\times$ tels que $p_i := u_i p'_i \in \mathbb{P}$. Posant $u = u_1^{-1} \cdot u_2^{-1} \cdots u_n^{-1} \in A^\times$ on obtient $a = u \cdot p_1 \cdot p_2 \cdots p_n$ qui a la forme requise.
Unicité : On fait une récurrence. Nous démontrons l'unicité pour les $0 \neq a \in A$ pouvant s'écrire avec au maximum n éléments de $\mathbb{P}$: $a = u \cdot p_1 \cdot p_2 \cdots p_n$. On suppose donc donnée une deuxième écriture de cette forme :

$$a = u \cdot p_1 \cdot p_2 \cdots p_n = v \cdot q_1 \cdot q_2 \cdots q_m$$

avec $u, v \in A^\times$, $n, m \in \mathbb{N}$ et $p_1, \ldots, p_n, q_1, \ldots, q_m \in \mathbb{P}$.
Cas $n = 0$: On a alors $a = u = v \cdot q_1 \cdot q_2 \cdots q_m$. Comme un produit d'éléments premiers n'est pas une unité, on a $m = 0$ et l'unicité est claire.
Supposons l'assertion démontrée pour $n - 1 \geq 0$, on va la démontrer pour n. Comme p_n divise $u \cdot p_1 \cdot p_2 \cdots p_n$, il s'en suit que p_n divise $v \cdot q_1 \cdot q_2 \cdots q_m$. Maintenant on utilise que p_n est un élément

premier et le lemme 4.7 pour obtenir un $j \in \{1, \dots, m\}$ tel que $p_n \mid q_j$. Comme q_j est irréductible, on a $p_n \sim q_j$, donc $p_n = q_j$ car $p_n, q_j \in \mathbb{P}$. On considère maintenant

$$\frac{a}{p_n} = u \cdot p_1 \cdot p_2 \cdots p_{n-1} = v \cdot q_1 \cdot q_2 \cdots q_{j-1} \cdot q_{j+1} \cdots q_m.$$

Cela nous permet d'utiliser l'hypothèse de récurrence qui nous donne $n - 1 = m - 1$ (donc $n = m$), ainsi qu'une identification entre $p_1, \dots, p_{n-1}$ et $q_1, \dots, q_{j-1}, q_{j+1}, \dots q_m$. Donc nous avons une identification entre $p_1, \dots, p_n$ et $q_1, \dots, q_m$. Cela achève la démonstration de l'unicité.
« (ii) $\Rightarrow$ (i) » : Il suffit de démontrer que tout élément irréductible $0 \neq p \in A \setminus A^\times$ est premier. Quitte à multiplier p par une unité (ce qui ne change pas la propriété d'être premier ou non) on peut supposer $p \in \mathbb{P}$. Soient donc $g, h \in A$ deux éléments tels que $p \mid gh$. Il existe alors $r \in A$ tel que $pr = gh$. On a $g = u \cdot p_1 \cdots p_n$ et $h = v \cdot q_1 \cdots q_s$ et $r = w \cdot \ell_1 \cdots \ell_t$ avec $u, v, w \in A^\times$, $n, s, t \in \mathbb{N}$ et $p_1, \dots, p_n, q_1, \dots, q_s, \ell_1, \dots, \ell_t \in \mathbb{P}$. L'égalité

$$pr = w \cdot p \cdot \ell_1 \cdots \ell_t = (u \cdot v) \cdot p_1 \cdots p_n \cdot q_1 \cdots q_s = gh$$

combinée avec l'unicité de l'écriture de (ii) implique que p est égal à p_i pour un $i \in \{1, \dots, n\}$ ou à q_j pour un $j \in \{1, \dots, s\}$. Donc, p divise g ou p divise h. Cela montre que p est premier. □

Le prochain but est de montrer que tout anneau principal est factoriel.

Lemme 5.5. *Soient A un anneau principal et $a_n \in A$ pour $n \in \mathbb{N}$ tels que*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \dots$$

Alors il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$ on a $(a_n) = (a_N)$. On dit que la chaîne d'idéaux devient stationnaire. En langage de l'algèbre commutatif on dit que tout anneau principal est « noethérien ».

Démonstration. Soit $I = \bigcup_{n \in \mathbb{N}} (a_n)$.
Nous montrons d'abord que I est un idéal de A : Soient $x, y \in I$ et $r \in A$. Il existe $i, j \in \mathbb{N}$ tel que $x \in (a_i)$ et $y \in (a_j)$. Soit $k = \max(i, j)$. Alors $x, y \in (a_k)$. Donc $x - y \in (a_k) \subseteq I$ et $rx \in (a_k) \subseteq I$, montrant $I \trianglelefteq A$.
Comme A est principal, il existe $a \in A$ tel que $I = (a)$. Comme I est la réunion de tous les (a_n) il existe $N \in \mathbb{N}$ tel que $a \in (a_N)$. Alors

$$I = (a) \subseteq (a_N) \subseteq (a_{N+1}) \subseteq (a_{N+2}) \subseteq \cdots \subseteq I$$

et la preuve est terminée. □

Lemme 5.6. *Soit A un anneau principal. Alors tout $0 \neq a \in A \setminus A^\times$ est divisible par un élément irréductible dans A.*

Démonstration. Supposons que c'est faux et que a n'est pas divisible par un élément irréductible (en particulier, a n'est pas lui-même irréductible).

- Alors $a = a_1 b_1$ avec $a_1, b_1 \in A \setminus A^\times$ qui ne sont pas divisibles par un élément irréductible. On a $(a) \subsetneq (a_1)$.

- Alors $a_1 = a_2 b_2$ avec $a_2, b_2 \in A \setminus A^\times$ qui ne sont pas divisibles par un élément irréductible. On a $(a) \subsetneq (a_1) \subsetneq (a_2)$.
- Alors $a_2 = a_3 b_3$ avec $a_3, b_3 \in A \setminus A^\times$ qui ne sont pas divisibles par un élément irréductible. On a $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3)$.
- ...

Continuant ainsi, nous obtenons une suite croissante d'idéaux qui n'existe pas par le lemme 5.5. □

Théorème 5.7. *Tout anneau principal est factoriel.*

Démonstration. La preuve est similaire à la preuve précédente. Par la proposition 4.16 et la définition d'anneau factoriel, il suffit de montrer que tout $0 \neq a \in A \setminus A^\times$ s'écrit comme un produit fini d'éléments irréductibles.

- Comme $a \notin A^\times$, par le lemme 5.6 il existe $0 \neq a_1 \in A \setminus A^\times$ irréductible et $b_1 \in A$ tels que $a = a_1 b_1$. Donc $(a) \subsetneq (b_1)$.
- Si $b_1 \notin A^\times$, par le lemme 5.6 il existe $0 \neq a_2 \in A \setminus A^\times$ irréductible et $b_2 \in A$ tels que $b_1 = a_2 b_2$. Donc $(a) \subsetneq (b_1) \subsetneq (b_2)$ et $a = a_1 a_2 b_2$.
- Si $b_2 \notin A^\times$, par le lemme 5.6 il existe $0 \neq a_3 \in A \setminus A^\times$ irréductible et $b_3 \in A$ tels que $b_2 = a_3 b_3$. Donc $(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq (b_3)$ et $a = a_1 a_2 a_3 b_3$.
- ...

Par le lemme 5.5, il existe $n \in \mathbb{N}$ tel que $b_n \in A^\times$. À ce moment-là on a $a = a_1 a_2 \cdots a_{n-1}(a_n b_n)$. La preuve est terminée car $a_n b_n$ est aussi irréductible. □

Corollaire 5.8. *Pour un anneau A nous avons les implications :*

$$A \text{ est euclidien } \Rightarrow A \text{ est principal } \Rightarrow A \text{ est factoriel } \Rightarrow A \text{ est intègre.}$$

Démonstration. Nous avons tout démontré dans les théorèmes 5.7 et 4.13. □

Valuations

Pour le reste de cette section, nous considérons un anneau factoriel A.

Définition 5.9. *Soient A un anneau factoriel et $\mathbb{P}$ un ensemble de représentants des éléments irréductibles dans A à association près (voir le lemme 5.3 pour des exemples). Nous pouvons réécrire l'assertion (ii) de la proposition 5.4 comme suit :*
Tout $x \in A \setminus \{0\}$ s'écrit comme un produit

$$x = u \cdot \prod_{p \in \mathbb{P}} p^{v_p(x)}$$

avec des uniques $u \in A^\times$, $v_p(x) \in \mathbb{N}_{\geq 0}$ et $v_p(x) = 0$ pour tous les $p \in \mathbb{P}$ sauf un nombre fini.
On pose $v_p(0) = \infty$.
On appelle la fonction $v_p : A \to \mathbb{N} \cup \{\infty\}$ la p-valuation *(ce qui explique le choix de la lettre v).*

Voici un exemple concret : Dans $A = \mathbb{Z}$ nous écrivons le nombre 84 comme $84 = 2^2 \cdot 3 \cdot 7$, c'est-à-dire $v_2(84) = 2$, $v_3(84) = 1$, $v_7(84) = 1$ et $v_p(84) = 0$ pour tout nombre premier $p \notin \{2, 3, 7\}$.
Dans un anneau factoriel, le pgcd et le ppcm existent toujours et ils sont très faciles et explicites.

Proposition 5.10. *Soient A un anneau factoriel, $\mathbb{P}$ un ensemble de représentants des éléments irréductibles dans A à association près et $0 \neq a, b \in A$.*

(a) $b \mid a \Leftrightarrow v_p(b) \leq v_p(a)$ *pour tout* $p \in \mathbb{P}$.

(b) $\prod_{p\in\mathbb{P}} p^{\min(v_p(a),v_p(b))}$ *est un* $\operatorname{pgcd}(a, b)$.

(c) $\prod_{p\in\mathbb{P}} p^{\max(v_p(a),v_p(b))}$ *est un* $\operatorname{ppcm}(a, b)$.

Démonstration. (a) « $\Rightarrow$ » : Il existe $c \in A$ tel que $a = bc$. Donc il existe des unités $u, v, w \in A^\times$ telles que

$$u \prod_{p\in\mathbb{P}} p^{v_p(a)} = \big(v \prod_{p\in\mathbb{P}} p^{v_p(b)}\big)\big(w \prod_{p\in\mathbb{P}} p^{v_p(c)}\big) = vw \prod_{p\in\mathbb{P}} p^{v_p(b)+v_p(c)}.$$

En conséquence $v_p(a) = v_p(b) + v_p(c)$ par l'unicité, donc $v_p(a) \geq v_p(b)$ pour tout $p \in \mathbb{P}$.
« $\Leftarrow$ » : Écrivons $a = u \prod_{p\in\mathbb{P}} p^{v_p(a)}$ et $b = v \prod_{p\in\mathbb{P}} p^{v_p(b)}$ avec $u, v \in A^\times$. Avec la définition $c := u/v \cdot \prod_{p\in\mathbb{P}} p^{v_p(a)-v_p(b)}$ nous avons $a = bc$, donc $b \mid a$.
(b) et (c) Exercice (utiliser (a) !). □

Lemme 5.11. *Soit A un anneau factoriel et $K = \operatorname{Frac}(A)$.*

(a) Nous savons que $\operatorname{pgcd}(a, b)$ *avec $a, b \in A$, $b \neq 0$ existe toujours. Toute fraction $\frac{a}{b} \in K$ possède un représentant $\frac{r}{s}$ tel que* $\operatorname{pgcd}(r, s) = 1$, *notamment $r = a/d$ et $s = b/d$ où d est un* $\operatorname{pgcd}(a, b)$. *Une telle fraction est dite* simplifiée ou irréductible (allemand : gekürzt).

(b) Soient $\frac{a}{b} = \frac{a'}{b'}$ toutes les deux simplifiées ($\operatorname{pgcd}(a, b) \sim \operatorname{pgcd}(a', b') \sim 1$*). Alors, $a \sim a'$ et $b \sim b'$.*

Démonstration. (a) C'est clair.
(b) De l'égalité $ab' = a'b$ nous déduisons $b \mid b'$ et $b' \mid b$, donc $b \sim b'$. Cela implique directement $a \sim a'$. □

Nous allons maintenant étendre la définition 5.9 au corps des fractions d'un anneau factoriel.

Définition-Lemme 5.12. *Soit A un anneau factoriel, $K = \operatorname{Frac}(A)$ et $\mathbb{P}$ un ensemble de représentants des éléments irréductibles dans A à association près. Tout $z \in K \setminus \{0\}$ s'écrit comme un produit*

$$z = u \cdot \prod_{p\in\mathbb{P}} p^{v_p(z)}$$

avec des uniques $u \in A^\times$, $v_p(z) \in \mathbb{Z}$ et $v_p(z) \neq 0$ seulement pour un nombre fini de $p \in \mathbb{P}$.

Illustrons d'abord la définition par un exemple concret :

$$\frac{-84}{30} = \frac{-2^2 \cdot 3^1 \cdot 7^1}{2^1 \cdot 3^1 \cdot 5^1} = -1 \cdot 2^1 \cdot 5^{-1} \cdot 7^1.$$

Notez que la fraction choisie s'écrit aussi comme $\frac{-14}{5}$ et comme $\frac{-14000}{5000}$, mais, on trouvera toujours la formule ci-dessus (c'est l'indépendance mentionnée à la fin de la preuve suivante).

Démonstration. On a $z = \frac{x}{y}$ et on utilise $x = u_1 \cdot \prod_{p\in\mathbb{P}} p^{v_p(x)}$ et $y = u_2 \cdot \prod_{p\in\mathbb{P}} p^{v_p(y)}$, dont on conclut

$$z = \frac{x}{y} = \frac{u_1}{u_2} \cdot \prod_{p\in\mathbb{P}} \frac{p^{v_p(x)}}{p^{v_p(y)}} = \frac{u_1}{u_2} \cdot \prod_{p\in\mathbb{P}} p^{v_p(x)-v_p(y)}$$

en utilisant les règles pour calculer avec les exposants. On pose évidemment $v_p(z) := v_p(x) - v_p(y)$. Notez qu'il faut encore vérifier que la définition ne dépend pas du choix de x et y. On vous laisse ceci comme exercice. □

Lemme 5.13. *Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$ et $\mathbb{P}$ un ensemble de représentants des éléments irréductibles dans A à association près.*

(a) Pour tous $x, y \in K$ et tout $p \in \mathbb{P}$ on a $v_p(xy) = v_p(x) + v_p(y)$. Pour que cette égalité ait un sens si $x = 0$ ou $y = 0$ nous admettons les égalités $a + \infty = \infty$ et $\infty + \infty = \infty$.

(b) On a : $x \in A \Leftrightarrow v_p(x) \geq 0 \; \forall\, p \in \mathbb{P}$.

(c) Soit $x \in A$. On a : $v_p(x) = 0$ pour tout $p \in \mathbb{P} \Leftrightarrow x \in A^\times$.

Démonstration. Exercice. □

6 Théorème de Gauß et critères d'irréductibilité de polynômes

Objectifs :

- Maîtriser la valuation de polynômes à coefficients dans un anneau factoriel ;
- connaître le lemme de Gauß concernant la valuation d'un produit de polynômes ;
- connaître le théorème de Gauß concernant la factorialité de l'anneau des polynômes à coefficient dans un anneau factoriel ainsi que la classification des éléments premiers ;
- connaître et savoir appliquer des critères d'irréductibilité comme le critère de réduction et le critère d'Eisenstein ;
- connaître des exemples et savoir démontrer des propriétés simples.

Pouvez-vous trouver un polynôme unitaire $g \in \mathbb{Q}[X]$ tel que $(X^2 + \frac{1}{2}X + 1) \cdot g(X) \in \mathbb{Z}[X]$? Plus généralement, est-ce qu'il existe des polynômes unitaires $f, g \in \mathbb{Q}[X]$ tels que $f(X) \cdot g(X) \in \mathbb{Z}[X]$, mais $f(X) \notin \mathbb{Z}[X]$ ou $g(X) \notin \mathbb{Z}[X]$? Dans cette section nous allons répondre à ces questions. En plus, nous allons étudier des critères simples pour montrer l'irréductibilité d'une grande classe de polynômes.
D'abord nous allons montrer l'assertion suivante démontrée par Gauß : si A est un anneau factoriel, alors l'anneau des polynômes $A[X]$ est aussi factoriel. Nous nous intéressons surtout au cas $A = \mathbb{Z}$, mais nous allons donner la démonstration en général (car c'est la même).
Nous insistons déjà au début sur le fait que l'anneau de polynômes $\mathbb{Z}[X]$ a une structure plus compliquée que $\mathbb{Q}[X]$ (ce qui peut étonner à première vue car c'est un sous-anneau). Nous savons déjà que $\mathbb{Z}[X]$ n'est pas un anneau principal (donc, pas un anneau euclidien non plus).

Une autre différence est que $\mathbb{Z}[X]$ possède plus d'éléments premiers. Pour être plus concret, considérons le polynôme constant $2 \in \mathbb{Z}[X]$. C'est clairement un élément irréductible de $\mathbb{Z}[X]$ (essayez de l'écrire comme un produit de deux polynômes $2 = f(X)g(X)$ avec $f, g \in \mathbb{Z}[X]$; vous trouverez tout de suite $f(X) = \pm 1$ ou $g(X) = \pm 1$). Puisque nous n'avons pas encore démontré que $\mathbb{Z}[X]$ est un anneau factoriel, nous ne savons pas encore que $2 \in \mathbb{Z}[X]$ est un élément premier. C'est un de nos buts. Voici l'idée : si 2 divise $f(X)g(X)$, alors il faut qu'on montre que soit les coefficients de $f(X)$, soit ceux de $g(X)$ sont pairs. Pour ceci, nous allons étudier la divisibilité des coefficients dans un produit de polynômes ; pour cela, nous allons introduire la valuation d'un polynôme et étudier comment elle se comporte dans des produits (voir la proposition 6.4).
Soulignons aussi que 2 et 1 ne sont pas associés dans $\mathbb{Z}[X]$, car les unités de cet anneau sont $\{1, -1\}$ (mais ces deux éléments sont associés dans $\mathbb{Q}[X]$ où tout élément non nul de $\mathbb{Q}$ est une unité – c'est un corps !) ; en particulier, l'idéal principal $2\mathbb{Z}[X] = \{2f(x) \mid f \in \mathbb{Z}[X]\}$, formé des polynômes dont tous les coefficients sont pairs, est strictement inclus dans $\mathbb{Z}[X]$ (l'idéal $2\mathbb{Q}[X]$ de $\mathbb{Q}[X]$ est évidemment égal à $\mathbb{Q}[X]$, car on peut diviser par 2).
Un autre type d'exemples d'éléments irréductibles dans $\mathbb{Z}[X]$ est le suivant : soit $f(X) \in \mathbb{Z}[X]$ un polynôme unitaire (plus bas, on va considérer la notion de « polynôme primitif » qui est un peu plus générale) qui est irréductible dans l'anneau $\mathbb{Q}[X]$. Nous allons voir qu'un tel polynôme est aussi un élément irréductible dans $\mathbb{Z}[X]$.
Notez qu'une condition comme « unitaire » ou « primitif » est nécessaire : le polynôme $2X + 2$ est irréductible dans $\mathbb{Q}[X]$, mais il ne l'est pas dans $\mathbb{Z}[X]$; en effet, on a $2X + 2 = 2 \cdot (X + 1)$ (rappelons encore une fois que 2 n'est pas une unité de $\mathbb{Z}[X]$).

Nous définissons maintenant une valuation pour les polynômes. Dans cette section, A est un anneau factoriel, K son corps des fractions et $\mathbb{P}$ un ensemble de représentants des éléments irréductibles dans A à association près.

Définition 6.1. *Soit* $f(x) = a_r X^r + a_{r-1} X^{r-1} + \cdots + a_1 X + a_0 \in K[X]$. *Pour* $p \in \mathbb{P}$ *on pose*

$$v_p(f) := \min_{i=0,\ldots,r} v_p(a_i)$$

et on l'appelle la p-valuation de f.
Le polynôme f *est appelé* primitif *si* $v_p(f) = 0$ *pour tout* $p \in \mathbb{P}$.

Voici des exemples concrets : $f(X) = X^2 + 2X + 4 \in \mathbb{Z}[X]$ est primitif. De même, tous les polynômes $f(X) \in A[X]$ unitaires sont primitifs. Le polynôme $f(X) = 10X^2 + 2X + 4 \in \mathbb{Z}[X]$ satisfait à $v_2(f) = 1$ et $v_p(f) = 0$ pour tout $2 \neq p \in \mathbb{P}$.

Lemme 6.2. *Soit* $0 \neq f \in K[X]$. *Alors :*

(a) On a que $v_p(f) \neq 0$ *seulement pour un nombre fini de* $p \in \mathbb{P}$.

(b) $v_p(f) \geq 0 \; \forall \, p \in \mathbb{P} \;\Leftrightarrow\; f \in A[X]$.

(c) Si $0 \neq f(X) = \sum_{i=0}^{r} a_i X^i \in A[X]$, *alors* $v_p(f) = v_p(\mathrm{pgcd}(a_0, a_1, \ldots, a_r))$ *pour tout* $p \in \mathbb{P}$.

(d) Il existe $a \in K \setminus \{0\}$ *tel que* $af \in A[X]$ *est un polynôme primitif.*

(e) Pour tout $a \in K \setminus \{0\}$ on a $v_p(af) = v_p(a) + v_p(f)$ pour tout $p \in \mathbb{P}$.

Démonstration. Exercice. □

Lemme 6.3. *L'application « réduction mod p » :*

$$\pi : A[X] \to A/(p)[X], \quad \sum_{i=0}^{r} a_i X^i \mapsto \sum_{i=0}^{r} \overline{a_i} X^i,$$

où $\overline{a_i}$ est la classe de a_i dans $A/(p)$, est un homomorphisme d'anneaux de noyau $\ker(\pi) = pA[X]$, l'ensemble de tous les polynômes dans $A[X]$ dont tout coefficient est divisible par p.

Démonstration. Clair. □

Dans ce lemme, nous réduisons les coefficients des polynômes modulo p. Par exemple, si $A = \mathbb{Z}$ et $p = 2$, alors, $\pi(X^3 + 7X^2 + 4X + 9) = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.

Proposition 6.4 (Lemme de Gauß)**.** *Soient $p \in \mathbb{P}$ et $f, g \in K[X]$. Alors, on a*

$$v_p(fg) = v_p(f) + v_p(g).$$

Démonstration. (1) Nous commençons par le cas spécial $f, g \in A[X]$ et $v_p(f) = 0$ et $v_p(g) = 0$ (et nous allons réduire l'étude générale à ce cas). L'argument est abstrait, mais très simple. On utilise π, la réduction modulo p, du lemme 6.3.

Les conditions $f \in A[X]$ et $v_p(f) = 0$ impliquent que $\pi(f) \neq 0 \in A/(p)[X]$ puisqu'il doit y avoir un coefficient de f qui ne se réduit pas en $\overline{0}$. Nous avons la même conclusion pour g, c'est-à-dire $\pi(g) \neq 0$.

Maintenant, utilisons le fait que p est un élément premier. Alors, (p) est un idéal premier de A, et en conséquence, $A/(p)$ est un anneau intègre. Alors, $0 \neq \pi(f)\pi(g)$ car $A/(p)[X]$ est aussi intègre par le corollaire 3.5.

Puisque π est un homomorphisme d'anneaux nous trouvons $0 \neq \pi(fg)$. Ceci implique que le polynôme $f(X)g(X)$ doit avoir un coefficient avec p-valuation 0, alors, on a démontré $v_p(fg) = 0$. On réécrit cette égalité comme la tautologie $v_p(fg) = 0 = 0 + 0 = v_p(f) + v_p(g)$.

(2) Soient maintenant $f, g \in K[X]$. Par le lemme 6.2 (d), il existe $a, b \in K$ tels que $\tilde{f} = af$ et $\tilde{g} = bg$ sont des polynômes primitifs dans $A[X]$. Nous avons donc

$$\begin{aligned} v_p(fg) = v_p(\frac{1}{a}\tilde{f}\frac{1}{b}\tilde{g}) &= v_p(\frac{1}{a}) + v_p(\frac{1}{b}) + v_p(\tilde{f}\tilde{g}) \\ &\overset{(1)}{=} v_p(\frac{1}{a}) + v_p(\frac{1}{b}) + v_p(\tilde{f}) + v_p(\tilde{g}) = v_p(\frac{1}{a}\tilde{f}) + v_p(\frac{1}{b}\tilde{g}) = v_p(f) + v_p(g). \end{aligned}$$

□

Corollaire 6.5. *Soient $f, g \in K[X]$ unitaires. Si $fg \in A[X]$, alors $f, g \in A[X]$.*

Démonstration. Puisque f, g sont unitaires, alors, fg l'est aussi. Soit $p \in \mathbb{P}$. En conséquence, on a

$$0 = v_p(fg) \overset{\text{Prop. 6.4}}{=} v_p(f) + v_p(g).$$

Le fait que f, g sont unitaires implique aussi $v_p(f), v_p(g) \leq 0$; donc, $v_p(f) = v_p(g) = 0$ pour tout $p \in \mathbb{P}$. Alors $f, g \in A[X]$. □

En d'autres mots, le corollaire dit que si le produit de deux polynômes unitaires n'a pas de dénominateur, alors chacun des deux polynômes n'a pas de dénominateur. Cela n'est pas si évident que ça !
Nous pouvons maintenant démontrer le théorème principal de cette section.

Théorème 6.6 (Gauß)**.** *(a) Soit A un anneau factoriel et K son corps des fractions. Soit $f \in A[X]$. Les deux assertions suivantes sont équivalentes :*

(i) f est premier dans $A[X]$.

(ii) f est d'une des deux formes suivantes :

(I) $f \in A$ (polynôme constant) et f est premier dans A.

(II) f est primitif et f est premier dans $K[X]$.

(b) Si A est un anneau factoriel, alors l'anneau des polynômes $A[X]$ est aussi un anneau factoriel.

Démonstration. (a) « $\Leftarrow$ » : Nous montrons d'abord que tout f de type (I) est en effet un élément premier de $A[X]$. Soit donc f un élément premier de A. Cela implique que $A/(f)$ et, en conséquence, aussi $A/(f)[X]$ sont des anneaux intègres. Nous utilisons l'application π « réduction mod f » du lemme 6.3 qui est clairement surjective. Donc le théorème d'isomorphisme implique que le quotient $A[X]/\ker(\pi)$ est isomorphe à l'anneau intègre $A/(f)[X]$, donc $\ker(\pi)$ est un idéal premier de $A[X]$. Un polynôme $g \in A[X]$ est dans le noyau de π si et seulement si tous ses coefficients sont divisibles par f. C'est-à-dire, $\ker(\pi) = (f) = f \cdot A[X] \lhd A[X]$. Donc, f est un élément premier de $A[X]$.
Montrons maintenant que tout f de type (II) est aussi un élément premier de $A[X]$. Soit $f \in A[X]$ primitif et élément premier de $K[X]$. On va vérifier la définition ; soient $g, h \in A[X]$ tels que $f \mid gh$. Lisons cette divisibilité dans $K[X]$; ceci implique que $f \mid g$ ou $f \mid h$ dans $K[X]$; disons, $f \mid g$ sans perte de généralité. On écrit cette divisibilité comme $g = fk$ avec $k \in K[X]$. On utilise la proposition 6.4 : $0 \leq v_p(g) = v_p(f) + v_p(k) = v_p(k)$ (puisque f est primitif : $v_p(f) = 0$ pour tout élément premier $p \in A$), donc $k \in A[X]$, alors la divisibilité $f \mid g$ est vraie dans $A[X]$. En conséquence, f est premier dans $A[X]$.
(b) Nous démontrons : tout $0 \neq f \in A[X]$ est un produit fini d'éléments premiers de type (I) ou (II). Cela implique en particulier que $A[X]$ est factoriel.
Choisissons $a \in K \setminus \{0\}$ tel que $g := \frac{1}{a} f \in A[X]$ est primitif par le lemme 6.2. On a $0 \leq v_p(a) = v_p(f)$, donc $a \in A \setminus \{0\}$. Puisque A est un anneau factoriel, nous écrivons $a = v \cdot \prod_{i=1}^{r} p_i$ avec $v \in A^\times$ et $p_1, \ldots, p_r$ des éléments premiers de A, c'est-à-dire, des éléments premiers de $A[X]$ de type (I). Puisque $K[X]$ est un anneau factoriel, nous pouvons écrire $g = w \cdot \prod_{i=1}^{s} h_i$ avec $w \in K[X]^\times = K^\times$ et $h_1, \ldots, h_r \in K[X]$ des polynômes irréductibles. Soit $a_i \in K^\times$ t.q. $\tilde{h}_i := a_i h_i \in A[X]$ est primitif

pour tout $1 \leq i \leq s$. Notez que les $\tilde{h}_i$ sont des éléments premiers de $A[X]$ de type (II). Posons $u = v \cdot w \cdot a_1^{-1} \cdot \ldots \cdot a_s^{-1} \in K^\times$. Encore par la proposition 6.4 on a :

$$0 = v_p(g) = v_p(w) + v_p(h_1 \cdots h_r) = v_p(w) - v_p(a_1 \cdots a_s) = v_p(u).$$

Donc, $u \in A^\times$ et on obtient l'assertion désirée :

$$f = ag = u \cdot p_1 \cdot \ldots \cdot p_r \cdot \tilde{h}_1 \cdot \ldots \cdot \tilde{h}_s.$$

(a) « $\Rightarrow$ » : Soit $f \in A[X]$ un élément premier (donc aussi irréductible). Par ce que nous venons de voir, f s'écrit comme un produit fini d'éléments premiers de type (I) ou (II). L'irréductibilité de f implique que ce produit n'a qu'un seul facteur qui est soit de type (I), soit de type (II). Ceci achève la démonstration de (a). □

Traitons le cas spécial qui nous intéressera le plus dans le corollaire suivant :

Corollaire 6.7. *Soit A un anneau factoriel et $f \in A[X]$ un polynôme primitif non constant. Alors, les assertions suivantes sont équivalentes :*

(i) f est irréductible dans $A[X]$;

(ii) f est premier dans $A[X]$;

(iii) f est premier dans $K[X]$;

(iv) f est irréductible dans $K[X]$.

Démonstration. Les équivalences « (i) $\Leftrightarrow$ (ii) » et « (iii) $\Leftrightarrow$ (iv) » proviennent du fait que $A[X]$ et $K[X]$ sont des anneaux factoriels. L'équivalence « (ii) $\Leftrightarrow$ (iii) » est une conséquence directe du théorème 6.6 (f doit être de type (II), car f est non constant). □

Le corollaire nous dit alors qu'un polynôme *unitaire* $f \in \mathbb{Z}[X]$ est irréductible si et seulement s'il est irréductible en tant que polynôme de $\mathbb{Q}[X]$. Le corollaire suivant est obtenu par une simple récurrence.

Corollaire 6.8. *Soit A un anneau factoriel et $n \in \mathbb{N}$. Alors, l'anneau $A[X_1, \ldots, X_n]$ est un anneau factoriel.*

Exemple 6.9. *L'anneau $\mathbb{Q}[X, Y]$ est factoriel, mais pas principal. Par exemple, l'idéal (X, Y) ne peut pas être engendré par un seul polynôme. Ceci donne un autre exemple d'anneau factoriel non principal.*

Nous allons maintenant prouver deux critères d'irréductibilité pour les polynômes : le critère de réduction et le critère d'Eisenstein.

Proposition 6.10 (Critère de réduction)**.** *Soit A un anneau factoriel et $f(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynôme primitif non constant. Pour un élément premier $p \in A$ nous considérons l'application π « réduction mod p » du lemme 6.3.*
Si p ne divise pas a_d et $\pi(f)$ est irréductible dans $A/(p)[X]$, alors f est irréductible dans $A[X]$.

Démonstration. Soit $f = gh$ avec $g, h \in A[X]$. Alors, on a $\pi(f) = \pi(gh) = \pi(g)\pi(h)$. Utilisons maintenant que $p \nmid a_d$. Écrivons $g(X) = \sum_{i=0}^{r} b_i X^i$ et $h(X) = \sum_{i=0}^{s} c_i X^i$ avec $b_r \neq 0 \neq c_s$. Puisque $a_d = b_r c_s$, on obtient que $p \nmid b_r$ et $p \nmid c_s$. Alors, le degré de $\pi(g)$ est égal au degré de g, et le degré de $\pi(h)$ est égal au degré de h. L'irréductibilité de $\pi(f)$ implique $\pi(g) \in A/(p)[X]^\times$ ou $\pi(h) \in A/(p)[X]^\times$. Comme p est premier, l'idéal $(p) \lhd A$ est premier et en conséquence $A/(p)$ est intègre. Donc $A/(p)[X]^\times = A/(p)^\times$, alors $\pi(g)$ ou $\pi(h)$ est constant. On obtient alors que soit g est constant, soit h l'est. Si g ou h était dans $A \setminus A^\times$, alors $f = gh$ ne serait pas primitif. Donc $g \in A^\times$ ou $h \in A^\times$. Cela finit la preuve. □

Exemple 6.11. *Considérons $f_1(X) = X^2 + X + 1 \in \mathbb{Z}[X]$, $f_2(X) = X^2 + 15X - 53 \in \mathbb{Z}[X]$, $f_3(X) = X^2 + 14X - 55 \in \mathbb{Z}[X]$ et $f_4(X) = X^2 + 15X - 54 \in \mathbb{Z}[X]$.*
Ces polynômes sont unitaires, donc primitifs. Noter que le polynôme $X^2 + X + 1 \in \mathbb{F}_2[X]$ est irréductible (pour les polynômes de degré au plus 3 il suffit de vérifier qu'il n'y a pas de racine – voir un exercice). Le critère de réduction modulo 2 montre alors que f_1 et f_2 sont irréductibles comme éléments de $\mathbb{Z}[X]$ (et aussi de $\mathbb{Q}[X]$). Cette argumentation ne s'applique pas à f_3. La réduction de f_3 modulo 3 est $X^2 + 2X + 2 \in \mathbb{F}_3[X]$ qui est irréductible ; alors, nous obtenons la même conclusion. Pour f_4 on ne peut ni utiliser la réduction modulo 2, ni modulo 3. En fait, aucun critère de réduction ne peut marcher puisqu'on a $X^2 + 15X - 54 = (X + 18)(X - 3)$.

Pour montrer que le critère de réduction s'applique très largement, nous allons maintenant interpréter l'évaluation d'un polynôme en une valeur (voir la définition 3.7) comme une réduction.

Remarque 6.12. *(a) Soient B un anneau, $A \subseteq B$ un sous-anneau et $b \in B$. Appliquant le théorème d'isomorphisme à l'évaluation, on obtient le homomorphisme d'anneau injectif*

$$\overline{\mathrm{ev}_b} : A[X]/(X - b) \to B, \quad f(X) \mapsto f(b).$$

Par cet isomorphisme, la réduction modulo l'idéal $(X - b)$ correspond donc à l'évaluation en b.

(b) Soit K un corps. Soit $A = K[T]$ (l'anneau des polynômes pour la variable T) et considérons un polynôme de la forme

$$f(T, X) = \sum_{i=0}^{d} a_i(T) X^i \in A[X].$$

Soit $b \in K$. L'idéal $T - b \in K[T]$ est maximal et premier (car $T - b$ est irréductible).

La réduction des coefficients $a_i(T)$ modulo $(T - b)$ revient par (a) à l'évaluation en b. Donc la réduction de $f(T, X)$ modulo $(T - b)$ n'est rien d'autre que le polynôme

$$f_b(X) := f(b, X) = \sum_{i=0}^{d} a_i(b) X^i \in K[X].$$

Exemple 6.13. *(a) On applique le remarque 6.12. Soit $f(T, X) \in A[X]$ pour $A = K[T]$ unitaire en la variable X. Si $f_b(X) := f(b, X)$ est irréductible dans $K[X]$ pour un $b \in K$, alors $f(T, X)$ est irréductible dans $A[X] = K[T, X]$.*

(b) Le polynôme $X^2 + X + 2TX + 5T^2X + T^3 + 1 \in \mathbb{Q}[T, X]$ est irréductible, puisqu'il est unitaire (pour la variable X) et $f(0, X) = X^2 + X + 1$ est irréductible.

Proposition 6.14 (Critère d'Eisenstein)**.** *Soit A un anneau factoriel et $f(X) = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynôme primitif non constant. Soit $p \in A$ un élément premier tel que*

$$p \nmid a_d, \quad p \mid a_i \text{ pour tout } 0 \le i \le d-1 \quad \text{et } p^2 \nmid a_0.$$

Alors, f est irréductible dans $A[X]$ (donc aussi irréductible dans $K[X]$).

Démonstration. Supposons le contraire et écrivons $f = gh$ avec $g(X) = \sum_{i=0}^{r} b_i X^i \in A[X]$, $h(X) = \sum_{i=0}^{s} c_i X^i \in A[X]$ non constants et $b_r \neq 0 \neq c_s$. À cause de $a_d = b_r c_s$, la condition $p \nmid a_d$ implique $p \nmid b_r$ et $p \nmid c_s$. À cause de $a_0 = b_0 c_0$, les conditions $p \mid a_0$ et $p^2 \nmid a_0$ impliquent sans perte de généralité que $p \mid b_0$ et $p \nmid c_0$.
Soit t le plus petit entier entre 1 et r tel que $p \nmid b_t$. Alors $1 \le t \le r < d$, puisque $p \mid b_0$ et $p \nmid b_r$. Nous posons $c_i = 0$ pour $i > s$ et on a :

$$\underbrace{a_t}_{\text{divisible par } p} = \underbrace{b_0 c_t + b_1 c_{t-1} + \cdots + b_{t-1} c_1}_{\text{divisible par } p} + \underbrace{b_t c_0}_{\text{non divisible par } p}.$$

Cette contradiction finit la preuve. □

Exemple 6.15.

(a) Considérons $f_1(X) = X^2 + 2X + 2 \in \mathbb{Z}[X]$ et $f_2(X) = X^7 + 72X^2 + 111X - 30 \in \mathbb{Z}[X]$. Ces polynômes sont unitaires, donc primitifs. Le critère d'Eisenstein avec $p = 2$ montre que f_1 est irréductible dans $\mathbb{Z}[X]$. L'irréductibilité de f_2 se montre par le critère d'Eisenstein avec $p = 3$.

(b) Soit p un nombre premier et $A = \mathbb{F}_p[T]$. Soit $f(T, X) = X^p - T \in A[X] = \mathbb{F}_p[T, X]$. En tant que polynôme irréductible, T est un élément premier de A. Le polynôme $f(T, X)$ satisfait aux conditions du critère d'Eisenstein en tant que polynôme dans la variable X pour l'élément premier T. Alors, $f(T, X)$ est irréductible.

Plus tard, ce polynôme nous servira comme exemple d'un polynôme irréductible, mais inséparable.

(c) Soit p un nombre premier. Considérons le polynôme $X^p - 1 \in \mathbb{Q}[X]$. Il n'est pas irréductible puisque nous avons :

$$X^p - 1 = (X-1)\underbrace{(X^{p-1} + X^{p-2} + \cdots + X + 1)}_{=:\Phi_p(X)} \in \mathbb{Z}[X].$$

On appelle $\Phi_p(X)$ le p-ième polynôme cyclotomique (en allemand : Kreisteilungspolynom)*. Il jouera un rôle important plus loin. Voici la preuve que $\Phi_p(X)$ est irréductible :*

Il suffit de montrer que $\Phi_p(X+1)$ est irréductible (car, si $\Phi_p(X+1) = f(X)g(X)$, alors, $\Phi_p(X) = f(X-1)g(X-1)$). On a

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} = \frac{\sum_{i=1}^{p} \binom{p}{i} X^i}{X} = X^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} X^{i-1},$$

qui est alors un polynôme d'Eisenstein pour l'élément premier p car $p \mid \binom{p}{i}$ pour tout $1 \le i \le p-1$ et $p^2 \nmid \binom{p}{1} = p$. Donc, $\Phi_p(X)$ est irréductible dans $\mathbb{Z}[X]$ (et alors aussi dans $\mathbb{Q}[X]$).

Complément : polynômes symétriques

Pour raison de temps, cette section ne sera probablement pas enseignée au cours. Elle peut servir comme référence.
Dans cette section, nous étudions l'anneau des polynômes en plusieurs variables. Plus particulièrement, on sera intéressé par les polynômes symétriques. Nous suivons le livre de Lang : Algebra.
Dans toute la section, soit A un anneau (commutatif, comme d'habitude). Considérons l'anneau des polynômes en n variables : $A[t_1, t_2, \ldots, t_n]$. Commençons par quelques calculs faciles.

- $(X - t_1)(X - t_2) = X^2 - (t_1 + t_2)X + t_1t_2$
- $(X - t_1)(X - t_2)(X - t_3) = X^3 - (t_1 + t_2 + t_3)X^2 + (t_1t_2 + t_1t_3 + t_2t_3)X - t_1t_2t_3$
- $(X - t_1)(X - t_2)(X - t_3)(X - t_4) = X^4 - (t_1 + t_2 + t_3 + t_4)X^3 + (t_1t_2 + t_1t_3 + t_1t_4 + t_2t_3 + t_2t_4 + t_3t_4)X^2 - (t_1t_2t_3 + t_1t_2t_4 + t_1t_3t_4 + t_2t_3t_4)X + t_1t_2t_3t_4$
- $(X - t_1)\cdots(X - t_n) = X^n - (t_1 + t_2 + \cdots + t_n)X^{n-1} + \cdots + (-1)^n t_1t_2\cdots t_n$

Définition 6.16. *Soient $s_1, \ldots, s_n \in A[t_1, \ldots, t_n]$ les polynômes définis par l'égalité*

$$\prod_{i=1}^{n}(X - t_i) = X^n + \sum_{i=1}^{n}(-1)^i s_i X^{n-i}.$$

Ces polynômes sont appelés polynômes symétriques élémentaires.

Définition 6.17. *(a) On appelle* monôme *tout élément de la forme $t_1^{e_1}t_2^{e_2}\ldots t_n^{e_n}$.*

Tout polynôme est donc une somme de monômes.

(b) Le degré (total) *du monôme $t_1^{e_1}t_2^{e_2}\ldots t_n^{e_n}$ défini comme $e_1 + e_2 + \cdots + e_n$.*

(c) Le degré (total) *d'un polynôme est défini comme le maximum des degrés des monômes apparaissant (avec coefficient non-zéro) dans le polynôme.*

(d) Un polynôme $f \in A[t_1, \ldots, t_n]$ est dit homogène de degré i *si le degré de tout monôme dans f est i.*

(e) Un polynôme $f \in A[t_1, \ldots, t_n]$ est dit symétrique *s'il est invariant par permutation des variables, c'est-à-dire, f est symétrique si et seulement si pour tout $\sigma \in S_n$ (le groupe symétrique) on a $f(t_{\sigma(1)}, t_{\sigma(2)}, \ldots, t_{\sigma(n)}) = f(t_1, t_2, \ldots, t_n)$.*

Lemme 6.18. *Soit $f \in A[t_1, \ldots, t_n]$ un polynôme homogène de degré i.*
Alors pour tout $\lambda, a_1, \ldots, a_n \in A$, on a $f(\lambda a_1, \lambda a_2, \ldots, \lambda a_n) = \lambda^i f(a_1, \ldots, a_n)$.

Démonstration. Exercice. □

Lemme 6.19. *Soient $s_1, \ldots, s_n \in A[t_1, \ldots, t_n]$ les polynômes symétriques élémentaires. Alors :*

(a) s_i est homogène de degré i pour tout $i = 1, \ldots, n$.

(b) s_i *est symétrique pour tout* $i = 1, \dots, n$.

Démonstration. Exercice. □

Définition 6.20. *Considérons* $A[X_1, \dots, X_n]$*, l'anneau des polynômes sur* A *en* n *variables qu'on appelle* $X_1, \dots, X_n$.

(a) Le poids *du monôme* $X_1^{\nu_1} X_2^{\nu_2} \dots X_n^{\nu_n}$ *est défini comme*

$$w(X_1^{\nu_1} X_2^{\nu_2} \dots X_n^{\nu_n}) = \nu_1 + 2\nu_2 + 3\nu_3 + \dots + n\nu_n.$$

(b) Le poids *d'un polynôme* $g \in A[X_1, \dots, X_n]$ *est le maximum des poids des monômes qui apparaissent dans* f.

Si $g \in A[X_1, \dots, X_n]$ est de poids d, alors le polynôme $g(s_1, \dots, s_n)$ est de degré d. En fait, cela est valable pour tous polynômes s_i de degré i en n'importe quel nombre de variables.

Théorème 6.21. *Soit* $f(t_1, \dots, t_n) \in A[t_1, \dots, t_n]$ *un polynôme symétrique de degré* d.
Alors il existe un polynôme $g(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$ *de poids inférieur ou égal à* d *tel que*

$$f(t_1, \dots, t_n) = g(s_1, \dots, s_n)$$

où $s_1, \dots, s_n \in A[t_1, \dots, t_n]$ *sont les polynômes symétriques élémentaires.*

Démonstration. La démonstration procède par une double récurrence : en n et en d. Le cas $n = 1$ est trivial pour tout d (tout polynôme est symétrique : $s_1 = t_1$).
Supposons le théorème vrai pour $n-1$, nous allons le montrer pour n, par récurrence en d.
Pour enlever une variable, nous allons (pour l'instant) remplacer t_n par 0.
Le polynôme $f(t_1, \dots, t_{n-1}, 0) \in A[t_1, \dots, t_{n-1}]$ est symétrique. C'est clair, mais donnons quand même un argument formel : soit $\sigma \in S_{n-1}$; nous le voyons comme élément de S_n en imposant $\sigma(n) = n$. Nous obtenons $f(t_{\sigma(1)}, \dots, t_{\sigma(n-1)}, t_n) = f(t_1, \dots, t_{n-1}, t_n)$, donc $f(t_{\sigma(1)}, \dots, t_{\sigma(n-1)}, 0) = f(t_1, \dots, t_{n-1}, 0)$.
Considèrons maintenant l'effet de $t_n = 0$ sur les polynômes symétriques élémentaires :

$$\begin{aligned}(X - t_1) \dots (X - t_{n-1})(X - 0) = X^n + \sum_{i=1}^{n} (-1)^i s_i(t_1, \dots, t_{n-1}, 0) X^{n-i} \\ = X \cdot \big(X^{n-1} + \sum_{i=1}^{n-1} (-1)^i s_i(t_1, \dots, t_{n-1}, 0) X^{n-i}\big)\end{aligned}$$

parce que $s_n(t_1, \dots, t_{n-1}, 0) = t_1 \cdot t_2 \cdots t_{n-1} \cdot 0 = 0$. De l'autre côté, nous avons

$$X \cdot (X - t_1) \dots (X - t_{n-1}) = X \cdot \big(X^{n-1} + \sum_{i=1}^{n-1} (-1)^i s_i(t_1, \dots, t_{n-1}) X^{n-i}\big),$$

d'où $s_i(t_1, \dots, t_{n-1}) = s_i(t_1, \dots, t_{n-1}, 0) =: \tilde{s_i}$ pour tout $i = 1, \dots, n-1$.

Faisons maintenant une récurrence en d. Le cas $d = 0$ des polynômes constants est trivial. Supposons le théorème montré pour les polynômes en n variables de degré $\leq d-1$, et soit $f(t_1, \ldots, t_n)$ de degré d. Soit $\tilde{f}(t_1, \ldots, t_{n-1}) := f(t_1, \ldots, t_{n-1}, 0)$. Par hypothèse de récurrence (pour la récurrence en n), il existe $\tilde{g} \in A[X_1, \ldots, X_{n-1}]$ de poids $\leq d$ tel que

$$\tilde{f}(t_1, \ldots, t_{n-1}) = \tilde{g}(s_1, \ldots, s_{n-1}).$$

Considérons le polynôme

$$f_1(t_1, \ldots, t_n) := f(t_1, \ldots, t_n) - \tilde{g}(s_1, \ldots, s_{n-1})$$

de degré $\leq d$ où $s_i = s_i(t_1, \ldots, t_n)$. Notons que f_1 est symétrique. Par le choix de $\tilde{g}$, nous avons

$$f_1(t_1, \ldots, t_{n-1}, 0) = \tilde{f}(t_1, \ldots, t_{n-1}) - \tilde{g}(s_1, \ldots, s_{n-1}) = 0.$$

Nous en déduisons que t_n divise f_1. La symétrie de f_1 implique que $t_1, \ldots, t_{n-1}$ divisent aussi f_1, donc $s_n = t_1 t_2 \cdots t_n$ divise f_1 :

$$f_1(t_1, \ldots, t_n) = s_n f_2(t_1, \ldots, t_n)$$

pour un polynôme $f_2 \in A[t_1, \ldots, t_n]$ de degré $\leq d - n < d$. En plus, f_2 est symétrique, car sinon f_1 ne le serait pas non plus. Par l'hypothèse de récurrence (pour la récurrence en d), il existe $g_2 \in A[X_1, \ldots, X_n]$ de poids $\leq d - n$ tel que

$$f_2(t_1, \ldots, t_n) = g_2(s_1, \ldots, s_n).$$

En tout, nous avons

$$f(t_1, \ldots, t_n) = \tilde{g}(s_1, \ldots, s_{n-1}) + s_n \cdot g_2(s_1, \ldots, s_n)$$

et le côté droit est de poids $\leq d$. □

Proposition 6.22. *Si $g \in A[X_1, \ldots, X_n]$ est un polynôme tel que $g(s_1, \ldots, s_n) = 0$, alors $g = 0$.*
On dit que les polynômes symétriques élémentaires sont algébriquement indépendants *(voir plus loin).*

Démonstration. Nous procédons encore par récurrence en n. Le cas $n = 1$ est trivial. Supposons la proposition démontrée pour $n-1$ variables, et démontrons-la pour n variables.
Supposons l'assertion fausse et prenons un $0 \neq g \in A[X_1, \ldots, X_n]$ de degré minimal en X_n tel que $g(s_1, \ldots, s_n) = 0$. Nous le considérons comme un élément de $(A[X_1, \ldots, X_{n-1}])[X_n]$:

$$g(X_1, \ldots, X_n) = g_0(X_1, \ldots, X_{n-1}) + g_1(X_1, \ldots, X_{n-1})X_n + \cdots + g_d(X_1, \ldots, X_{n-1})X_n^d.$$

Par la minimalité de g, on obtient que $g_0(X_1, \ldots, X_{n-1}) \neq 0$ (sinon g serait divisible par X_n, donc pas de degré minimal en X_n).
Remplaçons X_i par s_i :

$$0 = g(s_1, \ldots, s_n) = g_0(s_1, \ldots, s_{n-1}) + g_1(s_1, \ldots, s_{n-1})s_n + \cdots + g_d(s_1, \ldots, s_{n-1})s_n^d.$$

Imposons encore $t_n = 0$, on obtient (car $s_n(t_1, \ldots, t_{n-1}, 0) = t_1 t_2 \cdots t_{n-1} \cdot 0 = 0$)

$$0 = g_0(s_1, \ldots, s_{n-1})$$

où les s_i sont dans les variables $t_1, \ldots, t_{n-1}$. Par l'hypothèse de récurrence, on obtient $g_0 = 0$, une contradiction. □

Définition 6.23. *Soit* $f(X) = (X - t_1)(X - t_2)\cdots(X - t_n) \in A[t_1, \ldots, t_n][X]$. *Le* discriminant de f *est défini comme*

$$D_f = \prod_{1 \leq i < j \leq n} (t_i - t_j)^2.$$

Proposition 6.24. *(a) Soit* $f(X) = X^2 + bX + c \in A[X]$. *Alors* $D_f = b^2 - 4c$.

(b) Soit $f(X) = X^3 + aX + b \in A[X]$. *Alors* $D_f = -4a^3 - 27b^2$.

Démonstration. (a) Exercice.
(b) D_f est un polynôme homogène de degré 6 et symétrique dans les variables $t_1, \ldots, t_3$. Alors il existe un polynôme $g \in A[X_1, X_2, X_3]$ tel que

$$D_f = g(s_1, s_2, s_3).$$

Le fait que le coefficient de X^2 dans f est 0, implique $t_3 = -t_1 - t_2$. Nous substituons donc t_3 par $-t_1 - t_2$. Ecrivons $\tilde{s}_i(t_1, t_2) := s_i(t_1, t_2, -t_1 - t_2)$. On a $\tilde{s_1} = 0$, $a = \tilde{s_2}$ et $b = -\tilde{s_3}$. Nous avons

$$D_f = u\tilde{s}_2^3 + v\tilde{s}_3^2 = ua^3 - vb^3,$$

car D_f est homogène de degré 6.
Il reste à déterminer u, v. Nous faisons ceci en regardant deux polynômes bien choisis :

- $f_1(X) = X(X-1)(X+1) = X^3 - X$, donc $a = -1$ et $b = 0$, alors $D_{f_1} = -u$ et $D_f = 4$ (carré des différences des racines), donc $u = -4$.
- $f_2(X) = X^3 - 1$, donc $a = 0$ et $b = -1$, alors $D_{f_2} = v$. Les racines sont

  $$1, \frac{-1 + \sqrt{-3}}{2}, \frac{-1 - \sqrt{-3}}{2},$$

  donc

  $$D_{f_2} = (\frac{3}{2} - \frac{\sqrt{-3}}{2})^2 \cdot (\frac{3}{2} + \frac{\sqrt{-3}}{2})^2 \cdot (\sqrt{-3})^2 = (\frac{9}{4} - \frac{-3}{4})^2 \cdot (-3) = 9 \cdot -3 = -27.$$

Cela finit la démonstration. □

Complément : résultant

Pour raison de temps, cette section ne sera probablement pas enseignée au cours. Elle peut servir comme référence.
Dans la présentation des résultants, on suit le livre de Bosch. Soit K un corps. On pourrait remplacer le corps par n'importe quel anneau (commutatif) dans toute cette section. Nous ne le faisons pas pour raisons de simplicité.
On considère le K-espace vectoriel $K[X]_{<n} = \{f \in K[X] \mid \deg(f) < n\}$ de dimension n. Nous fixons la base $S_n = \{X^{n-1}, X^{n-2}, \ldots, X, 1\}$.

Définition 6.25. *Soient $f(X) = a_0X^m + a_1X^{m-1} + \cdots + a_{m-1}X + a_m$ et $g(X) = b_0X^n + b_1X^{n-1} + b_{n-1}X + b_n$ deux polynômes (on admet $a_0 = 0$ ou $b_0 = 0$). On définit l'application linéaire*

$$\Phi_{m,n}(f,g) : K[X]_{<n} \times K[X]_{<m} \to K[X]_{<n+m}, \quad (u,v) \mapsto (uf + vg).$$

Le résultant $\mathrm{res}_{m,n}(f,g)$ de (f,g) pour le degré formel (m,n) *est défini comme le déterminant (de la matrice qui – après choix de bases – représente) $\Phi_{m,n}(f,g)$.*
Si $\deg(f) = m$ et $\deg(g) = n$, on supprime souvent l'indice (m,n) et écrit seulement $\mathrm{res}(f,g)$.

Lemme 6.26. *On définit la matrice dans $\mathrm{Mat}_{n+m,n+m}(K)$*

$$R_{m,n}(f,g) := \begin{pmatrix} a_0 & a_1 & a_2 & \dots & \dots & a_m & & & \\ & a_0 & a_1 & a_2 & \dots & \dots & a_m & & \\ & & \ddots & \ddots & \ddots & & & \ddots & \\ & & & a_0 & a_1 & a_2 & \dots & \dots & a_m \\ b_0 & b_1 & b_2 & \dots & b_n & & & & \\ & b_0 & b_1 & b_2 & \dots & b_n & & & \\ & & \ddots & \ddots & \ddots & & \ddots & & \\ & & & \ddots & \ddots & \ddots & & \ddots & \\ & & & & b_0 & b_1 & b_2 & \dots & b_n \end{pmatrix},$$

où il y a n rangées dans la partie supérieure (celle avec les a_i) et m rangées dans la partie inférieure. Alors

$$M_{S_{n+m},S_n \sqcup S_m}\big(\Phi_{m,n}(f,g)\big) = \big(R_{m,n}(f,g)\big)^{\mathrm{tr}},$$

c'est-à-dire que la matrice qui représente l'application linéaire $\Phi_{m,n}(f,g)$ pour les bases S_{n+m} de $K[X]_{<n+m}$ et $S_n \sqcup S_m$ de $K[X]_{<n} \times K[X]_{<m}$ est la transposée de $R_{m,n}(f,g)$.
On a donc

$$\mathrm{res}_{m,n}(f,g) = \det\big(R_{m,n}(f,g)\big).$$

Démonstration. Vérification standard. □

On peut se demander pourquoi on ne définit pas $R_{m,n}(f,g)$ comme la transposée de la matrice que nous avons choisie ; on fait probablement ce choix pour des raisons historiques.

Exemple 6.27. *Soient $f(X) = X^2 + bX + c$ et $g(X) = f'(X) = 2X + b$. On a*

$$R_{2,1}(f,g) := \begin{pmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2 & b \end{pmatrix}.$$

Donc $\mathrm{res}_{2,1}(f,g) = -b^2 + 4c$.
On reconnaît donc le résultant comme le négatif du discriminant de f. Cela est un phénomène général, comme nous le verrons tout de suite.
C'est un bon exercice de calculer le résultant de $f(X) = X^3 + aX + b$ et $g(X) = f'(X) = 3X^2 + a$.

Proposition 6.28. *On garde la notation et on suppose $m+n \geq 1$. Alors il existe des polynômes $p \in K[X]_{\leq n}$ et $q \in K[X]_{<m}$ tels que* $\mathrm{res}_{m,n}(f,g) = pf + qg$.

Démonstration. Comme abréviation, nous écrivons $R = R_{m,n}(f,g)$. Soit $R^{\#}$ la matrice adjointe telle que

$$\mathrm{res}_{m,n}(f,g) \cdot \mathrm{id} = \det(R) \cdot \mathrm{id} = R \circ R^{\#}.$$

Le vecteur $e := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ est donc envoyé sur le vecteur qui représente le polynôme constant $\mathrm{res}_{m,n}(f,g)$ dans la base S_{m+n}. Donc le vecteur $R^{\#}e$ aussi y est envoyé par R. Ce vecteur $R^{\#}e$ représente un couple de polynômes $(p,q) \in K[X]_{<n} \times K[X]_{<m}$ dans la base $S_n \sqcup S_m$. Donc $\Phi_{m,n}(f,g)$ envoie (p,q) sur le polynôme constant $\mathrm{res}_{m,n}(f,g)$. □

Corollaire 6.29. *S'il existe $a \in K$ tel que $f(a) = g(a) = 0$, alors* $\mathrm{res}_{m,n}(f,g) = 0$.

On verra en bas que l'assertion réciproque est également vraie.

Démonstration. Le polynôme constant $\mathrm{res}_{m,n}(f,g)$ s'écrit comme $\mathrm{res}_{m,n}(f,g) = pf + qg$, donc $\mathrm{res}_{m,n}(f,g)$ est en particulier égal à $p(a)f(a) + q(a)g(a) = 0$. □

Définition 6.30. *Le déterminant de l'application linéaire*

$$\mu_f(g) : K[X]/(f) \to K[X]/(f), \quad v + (f) \mapsto gv + (f)$$

s'appelle la norme *de g (par rapport à f). Notation : $N_f(g)$*

Lemme 6.31. *Soient $f, g \in K[X]$ non-zéro. Alors les assertions suivantes sont équivalentes :*

(i) $\mathrm{pgcd}(f,g) = 1$

(ii) $\mu_f(g)$ *est inversible.*

(iii) $N_f(g) \neq 0$

Démonstration. L'équivalence de (ii) et (iii) provient du fait qu'un endomorphisme linéaire est inversible si et seulement si son déterminant est non-zéro.
Si (i) est vrai, la relation de Bézout nous donne des polynômes $u, v \in K[X]$ tels que $1 = uf + vg$; donc $\mu_f(g)$ est inversible avec inverse $\mu_f(v)$; cela montre (ii).
Si (ii) est vrai, alors $\mu_f(g)$ est surjectif, donc il existe $v \in K[X]$ tel que $vg + (f) = 1 + (f)$; cela revient à dire qu'il existe $u \in K[X]$ tel que $1 = uf + vg$. Si $h \in K[X]$ divise f et g, alors h divise 1. Alors le $\mathrm{pgcd}(f,g)$ est 1, donc (i) est vrai. □

Lemme 6.32. *(a) Pour $g_1, g_2 \in K[X]$ on a $N_f(g_1 g_2) = N_f(g_1) \cdot N_f(g_2)$.*

(b) Supposons f de degré m. L'application $\alpha_f : K[X]/(f) \to K[X]_{<m}$ qui envoie la classe $h + (f)$ sur le reste dans la division euclidienne de h par f est un isomorphisme de K-espaces vectoriels. Donc les classes $\alpha_f^{-1}(X^{m-1}) = X^{m-1} + (f), \alpha_f^{-1}(X^{m-2}) = X^{m-2} + (f), \ldots, \alpha_f^{-1}(X) = X + (f), \alpha_f^{-1}(1) = 1 + (f)$ forment une K-base T_f de $K[X]/(f)$. On a $M_{S_m,S_m}(\alpha_f \circ \mu_f(g) \circ \alpha_f^{-1}) = M_{T_f,T_f}(\mu_f(g))$.

(c) Pour tout $g \in K[X]$ et tout $\alpha \in K$ on a $N_{X-\alpha}(g) = g(\alpha)$.

Démonstration. (a) C'est la multiplicativité du déterminant.
(b) Il faut d'abord remarquer que α_f est bien défini : si h_1, h_2 représentent la même classe $h_1 + (f) = h_2 + (f)$, alors le reste de h_1 et de h_2 est le même, donc $\alpha_f(h_1 + (f)) = \alpha_f(h_2 + (f))$ ne dépend pas du choix de représentants. La K-linéarité de α est facile à vérifier. Si $\alpha_f(h) = 0$, alors le reste est zéro et h est divisible par f. Cela montre l'injectivité. Si h est de degré $< m$, alors h est égal à son reste, donc α_f est aussi surjectif.
(c) Le reste de g dans la division euclidienne par $X - \alpha$ est égal à $g(\alpha)$. Il y a plusieurs manières pour le voir : on peut par exemple voir que $X^n - \alpha^n$ est divisible par $(X - \alpha)$, donc $g(X) - g(\alpha)$ est divisible par $(X - \alpha)$. En conséquence, μ_{X_α} est la multiplication par $g(\alpha)$ (et $K[X]/(X - \alpha)$ est de dimension 1), donc le déterminant est égal à $g(\alpha)$. □

Lemme 6.33. *Supposons f unitaire de degré m.*

(a) Pour tout $n \geq 1$, considérons l'application

$$\Psi : K[X]_{<n} \times K[X]_{<m} \to K[X]_{<m+n}, \quad (u, v) \mapsto fu + v.$$

Alors la matrice $C := M_{S_{n+m}, S_n \sqcup S_m}(\Psi)$ est triangulaire inférieure avec 1 sur la diagonale. Donc son déterminant est 1. En plus, Ψ est inversible et son inverse est décrit par C^{-1} qui est aussi de déterminant 1.

(b) Pour tout $g \in K[X]$ et tout $n \geq \deg(g)$, considérons maintenant l'application composée

$$\Theta : K[X]_{<n} \times K[X]_{<m} \xrightarrow{\Phi_{m,n}(f,g)} K[X]_{<m+n} \xrightarrow{\Psi^{-1}} K[X]_{<n} \times K[X]_{<m}.$$

Elle envoie (u, v) sur $(u + u', v')$ où $vg = u'f + v'$ avec $\deg(v') < m$ (division euclidienne). La matrice $M_{S_n \sqcup S_m, S_n \sqcup S_m}(\Theta)$ s'écrit en blocs comme

$$\begin{pmatrix} \boxed{\mathrm{id}_n} & \boxed{**} \\ \boxed{0} & \boxed{M} \end{pmatrix}$$

où $M = M_{T_f, T_f}(\mu_f(g))$ est la matrice qui représente $\mu_f(g)$ dans la base T_f.

Démonstration. (a) Application des règles pour écrire $M_{S_{n+m}, S_n \sqcup S_m}(\Psi)$.
(b) L'application Θ est facilement décrite explicitement comme énoncé. Pour voir que le bloc en haut à gauche est bien id_n, il suffit de voir que $(X^i, 0)$ est envoyé sur $(X^i, 0)$ pour $0 \leq i < n$. Pour voir le bloc en bas à droite, on utilise que $v' \equiv gv \mod (f)$. Le reste est une application des règles selon lesquelles décrire les matrices qui représentent une application linéaire. □

Lemme 6.34. *(a)* $\mathrm{res}_{m,n}(f, g) = (-1)^{mn} \cdot \mathrm{res}_{n,m}(g, f)$

(b) Pour tout $a, b \in K$ on a $\mathrm{res}_{m,n}(af, bg) = a^n b^m \cdot \mathrm{res}_{m,n}(f, g)$.

Démonstration. Règles pour déterminants. □

Corollaire 6.35. *(a) Pour tout f unitaire de degré m, pour tout $g \in K[X]$ et pour tout $n \geq \deg(g)$, on a*

$$N_f(g) = \mathrm{res}_{m,n}(f,g) = \mathrm{res}_{\deg(f),\deg(g)}(f,g) = \mathrm{res}(f,g).$$

(b) Pour tout $f \in K[X]$ et pour tout $g_1, g_2 \in K[X]$ on a

$$\mathrm{res}(f, g_1 g_2) = \mathrm{res}(f, g_1) \cdot \mathrm{res}(f, g_2).$$

(c) Pour tout $f_1, f_2 \in K[X]$ et pour tout $g \in K[X]$ on a

$$\mathrm{res}(f_1 f_2, g) = \mathrm{res}(f_1, g) \cdot \mathrm{res}(f_2, g).$$

(d) Pour tous $f, g \in K[X]$ on a

$$\mathrm{res}(f,g) \neq 0 \Leftrightarrow \mathrm{pgcd}(f,g) = 1.$$

En particulier, si $f = a \cdot \prod_{i=1}^{m}(X - \alpha_i)$ et $g = b \cdot \prod_{j=1}^{n}(X - \beta_j)$, alors

$$\mathrm{res}(f,g) \neq 0 \Leftrightarrow \forall\, 1 \leq i \leq m, \forall\, 1 \leq j \leq n : \alpha_i \neq \beta_j.$$

(e) Soit $f = \prod_{i=1}^{m}(X - \alpha_i) \in K[X]$. Alors pour tout $g \in K[X]$ on a

$$\mathrm{res}(f,g) = \prod_{i=1}^{m} g(\alpha_i).$$

(f) Soient $f = a \cdot \prod_{i=1}^{m}(X - \alpha_i)$ et $g = b \cdot \prod_{j=1}^{n}(X - \beta_j)$ des polynômes dans $K[X]$. Alors

$$\mathrm{res}(f,g) = a^n b^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

Démonstration. (a) Par le lemme 6.33 et les règles du déterminant, on a

$$\begin{aligned} N_f(g) = \det\left(M_{T_f,T_f}(\mu_f(g))\right) &= \det\left(M_{S_n \sqcup S_m, S_n \sqcup S_m}(\Theta)\right) \\ &= \det\left(M_{S_{n+m}, S_n \sqcup S_m}(\Psi^{-1})\right) \cdot \det\left(R_{m,n}(f,g)\right) = \mathrm{res}_{m,n}(f,g). \end{aligned}$$

(b) Cela suit de (a).
(c) On utilise le lemme 6.34(a) et fait le calcul

$$\begin{aligned} \mathrm{res}(f_1 f_2, g) &= (-1)^{(\deg(f_1)+\deg(f_2))\deg(g)} \cdot \mathrm{res}(g, f_1 f_2) \\ &= (-1)^{(\deg(f_1)+\deg(f_2))\deg(g)} \cdot \mathrm{res}(g, f_1) \cdot \mathrm{res}(g, f_2) \\ &= (-1)^{\deg(f_1)\deg(g)} \cdot \mathrm{res}(g, f_1) \cdot (-1)^{\deg(f_2)\deg(g)} \mathrm{res}(g, f_2) \\ &= \mathrm{res}(f_1, g) \cdot \mathrm{res}(f_2, g). \end{aligned}$$

(d) Cela suit de (a) avec le lemme 6.31.
(e) D'abord on voit par (a) et le lemme 6.32 que $\mathrm{res}(X - \alpha, g) = g(\alpha)$. Par (c) et récurrence, cela entraîne l'assertion.
(f) Conséquence directe de (e). □

Finalement, le résultant nous donne une procédure explicite pour calculer le discriminant d'un polynôme.

Corollaire 6.36. *Soit $f = \prod_{i=1}^{m}(X - \alpha_i) \in K[X]$. Dans la définition 6.23 nous avons défini le discriminant de f.*
Si on note par f' la dérivée de f, alors on a

$$D_f = (-1)^{m(m-1)/2} \cdot \mathrm{res}(f, f').$$

Démonstration. La règle de Leibniz pour le calcul de la dérivée d'un produit de polynômes connue des cours d'analyses est aussi valable sur n'importe quel corps (calcul facile). Donc nous obtenons

$$f'(X) = \sum_{k=1}^{m} \prod_{j=1, j\neq k}^{m} (X - \alpha_j).$$

Nous avons donc $f'(\alpha_i) = \prod_{j=1, j\neq i}^{m}(\alpha_i - \alpha_j)$. Par le corollaire 6.35(e) nous déduisons

$$\mathrm{res}(f, f') = \prod_{i=1}^{m} \prod_{j=1, j\neq i}^{m} (\alpha_i - \alpha_j).$$

Si on compare ce produit avec celui dans la définition du discriminant, c'est-à-dire,

$$D_f = \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2,$$

on obtient le facteur $(-1)^{m(m-1)/2}$ qui provient du fait qu'à chaque fois que $i > j$ on doit multiplier $(\alpha_i - \alpha_j)$ par (-1). □

7 Extensions de corps

Objectifs :

- Maîtriser la caractéristique d'un anneau,
- connaître le corps premier d'un corps, et le Frobenius dans les corps de caractéristique positif,
- connaître la définition d'une extension de corps et de son degré,
- savoir appliquer les propositions importantes,
- connaître des exemples et savoir démontrer des propriétés simples.

Rappelons d'abord la convention : **Tout corps est supposé commutatif pour la suite du cours.**

Caractéristique

Définition 7.1. *Soit A un anneau. Pour $n \in \mathbb{N}_{\geq 1}$, on écrit*

$$n_A := n \cdot 1_A := \underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}} \in A.$$

On distingue deux cas :

(I) Il n'existe pas de $n \in \mathbb{N}_{\geq 1}$ tel que $n_A = 0 \in A$. Dans ce cas, on dit que la caractéristique de A est 0.

(II) Il existe $n \in \mathbb{N}_{\geq 1}$ tel que $n_A = 0 \in A$. Soit $t \in \mathbb{Z}_{>0}$ l'entier positif minimal ayant cette propriété. Dans ce cas, on dit que la caractéristique de A est t.

On utilise la notation $\mathrm{car}(A)$ pour la caractéristique.

Exemple 7.2. *(a)* $\mathrm{car}(\mathbb{C}) = \mathrm{car}(\mathbb{Z}) = \mathrm{car}(\mathbb{Q}) = \mathrm{car}(\mathbb{R}) = 0$.

(b) Soit $n \in \mathbb{Z}_{\geq 1}$. On a $\mathrm{car}(\mathbb{Z}/n\mathbb{Z}) = n$.

Lemme 7.3. *Soit A un anneau de caractéristique $\mathrm{car}(A) = p$.*

(a) Il existe un unique homomorphisme d'anneaux $\varphi_A : \mathbb{Z} \to A$. On a $\varphi_A(n) = n_A$ pour tout $n \in \mathbb{Z}$ où on étend la définition de n_A ainsi : $0_A = 0$ et $n_A = -(|n|_A)$ pour $n < 0$.

(b) $\ker(\varphi_A) = (p)$.

(c) Si A est intègre et $p > 0$, alors p est un nombre premier.

Le lemme caractérise la caractéristique comme l'unique nombre naturel qui engendre $\ker(\varphi_A)$.

Démonstration. (a) Il est clair que φ_A est un homomorphisme d'anneaux. Si $\varphi : \mathbb{Z} \to A$ est un homomorphisme d'anneaux, on a $\varphi(1) = 1_A$, donc

$$\varphi(n) = \varphi(\underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}}) = \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_{n \text{ fois}} = \underbrace{1_A + 1_A + \cdots + 1_A}_{n \text{ fois}} = n_A$$

pour $n \geq 0$ et donc $\varphi = \varphi_A$, montrant l'unicité.
(b) Comme $\mathbb{Z}$ est un anneau principal, le noyau de φ_A est engendré par un seul élément q. Puisque $\mathbb{Z}^\times = \{\pm 1\}$, on peut supposer $q \geq 0$. Nous savons que $q = 0$ si et seulement si φ_A est injectif. On se trouve donc dans le cas (I) de la définition 7.1 (la caractéristique de A est 0) si et seuelement si $q = 0$. Soit maintenant $q > 0$. Si $t \in \mathbb{Z}_{>0}$ satisfait $\varphi_A(t) = 0$, on a $q \mid t$ et donc $t \geq q$. Il en suit que la caractéristique de A est q. Dans les deux cas, on trouve $p = q$.
(c) Si A est un anneau intègre, l'image de φ_A, qui est un sous-anneau de A, est aussi un anneau intègre. Le théorème d'isomorphisme nous dit $A/\ker(\varphi_A) \cong \mathrm{im}(\varphi_A)$. Donc $\ker(\varphi_A)$ est un idéal premier de $\mathbb{Z}$, d'où p est soit 0, soit un nombre premier. □

Lemme 7.4. *(a) Soit $\varphi : A \to B$ un homomorphisme injectif d'anneaux. Alors,* $\mathrm{car}(A) = \mathrm{car}(B)$.

(b) Soient K, L deux corps de caractéristiques différentes. Il n'existe pas d'homomorphisme de corps $\varphi : K \to L$.

(c) Soit A un anneau intègre et $K := \mathrm{Frac}(A)$ son corps des fractions. Alors, $\mathrm{car}(A) = \mathrm{car}(K)$.

Démonstration. (a) La composée $\mathbb{Z} \xrightarrow{\varphi_A} A \xrightarrow{\varphi} B$ est égale à φ_B. Puisque φ est injectif, on a $\ker(\varphi_A) = \ker(\varphi_B)$, donc $\mathrm{car}(A) = \mathrm{car}(B)$.
(b) Des homomorphismes entre corps sont injectifs car le noyau est un idéal premier, donc (0).
(c) Le plongement naturel $A \to K$ donné par $a \mapsto \frac{a}{1}$ est injectif, donc on peut utiliser (a). □

Pour voir que les conditions dans (a) sont nécessaires, on peut regarder la projection naturelle $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{F}_p$ et remarque $\mathrm{car}(\mathbb{Z}) = 0 \neq p = \mathrm{car}(\mathbb{F}_p)$. Pour illustrer (b), on peut conclure qu'il n'existe aucun homomorphisme d'anneaux entre $\mathbb{Q}$ et $\mathbb{F}_p$ (dans les deux senses), ni entre $\mathbb{F}_p$ et $\mathbb{F}_q$ si p, q sont tous les deux premiers.

Définition 7.5. *Soit K un corps. On appelle* corps premier de K *(en anglais :* prime field*; en allemand :* Primkörper*) le plus petit sous-corps contenu dans K.*

L'existence du plus petit sous-corps est justifiée par le prochain lemme.

Lemme 7.6. *(a) Soit A un anneau intègre de caractéristique $p > 0$. Alors il existe un homomorphisme d'anneaux injectif $\overline{\varphi}_A : \mathbb{F}_p \to A$. Donc $\mathbb{F}_p$ est le corps premier de tout corps de caractéristique $p > 0$.*

(b) $\mathbb{Q}$ est le corps premier de tout corps K de caractéristique 0.

Démonstration. (a) Le théorème d'isomorphisme nous dit que φ_A induit l'application récherchée dont nous identifions l'image à $\mathbb{F}_p$.
(b) Dans ce cas, φ_K est injectif car son noyau est (0) par la caractérisation de la caractéristique. Donc K contient $\mathbb{Z}$ (plus précisement l'image de $\mathbb{Z}$ par φ_K qui est isomorphe à $\mathbb{Z}$). Comme K est un corps, il contient aussi les fractions de $\mathbb{Z}$, donc $\mathbb{Q}$. □

Définition-Lemme 7.7. *(a) Soit A un anneau intègre de caractéristique $p > 0$. On définit l'application*

$$\mathrm{Frob} : A \to A, \quad x \mapsto x^p,$$

dite « homomorphisme de Frobenius ». C'est un homomorphisme d'anneaux.

(b) Si K est un corps fini de caractéristique $p > 0$, alors Frob *est un automorphisme de K (par définition, un automorphisme de K est un isomorphisme de K dans lui-même).*

Démonstration. (a) La seule chose qui doit être démontrée est l'additivité :

$$\mathrm{Frob}(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p.$$

On utilise que $p \mid \binom{p}{i}$ pour tout $1 \leq i \leq p-1$.
(b) Les homomorphismes de corps sont injectifs. Puisque le nombre d'éléments de K est fini, Frob est bijectif. □

Proposition 7.8 (« Petit Fermat »)**.** *Soit p un nombre premier. Alors pour tout $x \in \mathbb{F}_p$, on a* $\mathrm{Frob}(x) = x^p = x$.

Démonstration. C'est une conséquence du « petit théorème de Fermat pour groupes » démontré dans le cours « structures mathématiques ». Il dit que si on élève un élément d'un groupe de cardinal n à la n-ième puissance, alors on obtient l'élément neutre. Nous appliquons ce résultat au groupe multiplicatif $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ de cardinal $p-1$. Explicitement, cela veut dire que pour $x \in \mathbb{F}_p \setminus \{0\}$, on a $x^{p-1} = 1$, donc, $x^p = x$. Cette égalité est trivialement satisfaite pour $x = 0$ aussi. □

Proposition 7.9. *Soit K un corps. Soit $f \in K[X]$ un polynôme.*

(a) Si $f(a) = 0$ pour un $a \in K$, alors $f(X) = (X-a)g(X)$ pour un $g \in K[X]$.

(b) Si le degré de f est $d \geq 0$, alors f possède au plus d zéros.

La conclusion de la proposition reste valable si on remplace K par un anneau intègre. Par contre, l'intégrité est nécessaire car, par exemple, le polynôme $X^2 - \overline{1} \in \mathbb{Z}/12\mathbb{Z}$ possède les zéros $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

Démonstration. (a) On utilise la division euclidienne :

$$f(x) = (X-a)g(X) + r(X)$$

où $g, r \in K[X]$ et $\deg(r) < \deg(X-a) = 1$, d'où $r(X) = b$ est constant pour un $b \in K$. Nous avons $0 = f(a) = (a-a)g(a) + b = b$.
(b) Par récurrence. Si $d = 0$, alors $f(X) = b \neq 0$ est constant et ne possède donc aucun zéro. Si $f(X)$ est de degré $d > 0$ et si $f(a) = 0$ pour un $a \in K$, alors par (a) nous avons $f(X) = (X-a)g(X)$ où $g(X)$ est de degré $d-1$ et – par l'hypothèse de récurrence – possède donc au plus $d-1$ zéros. Alors, si $f(b) = 0$, par le fait que le seul diviseur de zéro dans le corps K est 0, on a soit $b - a = 0$ (donc $a = b$), soit $g(b) = 0$. Cela montre que f ne possède pas plus que d zéros. □

Proposition 7.10. *Soit K un corps de caractéristique $p > 0$. Alors, l'image de $\overline{\varphi}_K : \mathbb{F}_p \to K$ est égale à l'ensemble $\{x \in K \mid \mathrm{Frob}(x) = x^p = x\}$.*

Démonstration. Par la proposition 7.9, le polynôme $X^p - X \in K[X]$ possède au plus p zéros. A cause du petit Fermat 7.8, nous en connaissons déjà p : les éléments $\overline{\varphi}_K(x)$ pour $x \in \mathbb{F}_p$. Si on interprète l'ensemble $\{x \in K \mid \mathrm{Frob}(x) = x^p = x\}$ comme l'ensemble des zéros dans K de $X^p - X \in K[X]$, la preuve est complète. □

Extensions

Lemme 7.11. *Soit A un anneau qui contient un corps $K \subseteq A$ comme sous-anneau. On définit une multiplication scalaire de K sur A comme la multiplication dans A, c'est-à-dire pour $x \in K$ et $a \in A$, on prend $x \cdot a \in A$ (possible car $x \in K \subseteq A$). Cela munit A d'une structure de K-espace vectoriel.*

Démonstration. C'est trivial car les axiomes pour l'espace vectoriel font partie des axiomes pour un corps. □

Définition 7.12. *(a) Soit L un corps et $K \subseteq L$ un sous-corps. Dans ce cas on dit que L est* une extension du corps K *(ou bien que L/K est une* extension de corps*).*

(b) Si $K \subseteq L$ est une extension de corps, alors par le lemme 7.11, L est un K-espace vectoriel.

Le degré *de l'extension de corps L/K est défini comme*

$$[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}.$$

Si $[L : K] < \infty$ on parle d'une extension finie de corps *(attention : ne pas confondre avec extension de corps finis !).*

Un exemple important est l'extension $\mathbb{R} \subset \mathbb{C}$ (ou bien $\mathbb{C}/\mathbb{R}$). Le corps des nombres complexes $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel de dimension 2 (une $\mathbb{R}$-base est donnée par $1, i = \sqrt{-1}$), donc $[\mathbb{C} : \mathbb{R}] = 2$.

Corollaire 7.13. *(a) Le cardinal de tout corps fini est une puissance d'un nombre premier.*

(b) Si L/K est une extension de corps finis et $\#K = p^a$ et $\#L = p^b$ pour un nombre premier p et $a, b \in \mathbb{N}$, alors $a \mid b$.

Démonstration. (a) Soit K un corps de cardinal $n \in \mathbb{N}$. Sa caractéristique est un nombre premier p et $\mathbb{F}_p$ est son corps premier. Donc nous avons une extension de corps $K/\mathbb{F}_p$. Donc K est un $\mathbb{F}_p$-espace vectoriel de dimension finie r. Alors $n = \#K = p^r$.
(b) Puisque L est un K-espace vectoriel de dimension finie d, on a $p^b = \#L = (\#K)^d = (p^a)^d = p^{ad}$, d'où $b = da$. □

Proposition 7.14 (Multiplicativité du degré)**.** *Soient $K \subseteq L \subseteq M$ des extensions de corps. Alors,*

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

Démonstration.

- M/L et L/K sont finis : En tant que K-espaces vectoriels on a $L \cong K^{[L:K]}$ (car tout K-espace vectoriel de dimension d est isomorphe à K^d). De la même façon : $M \cong L^{[M:L]}$ en tant que L-espaces vectoriels (donc aussi en tant que K-espaces vectoriels). Donc on a des isomorphismes de K-espaces vectoriels :

$$K^{[M:K]} \cong M \cong L^{[M:L]} \cong (K^{[L:K]})^{[M:L]} = K^{[L:K]\cdot[M:L]}.$$

- M/L infini : Il existe un ensemble infini d'éléments $m_1, m_2, \ldots \in M$ qui sont L-linéairement indépendants, donc aussi K-linéairement indépendants. Donc $[M : K] = \infty$.

- L/K infini : Comme $M \supseteq L$ on a $\dim_K(M) \geq \dim_K(L) = \infty$.

□

Par la multiplicativité du degré, nous obtenons une deuxième démonstration du corollaire 7.13 (b) : $b = [L : \mathbb{F}_p] = [L : K] \cdot [K : \mathbb{F}_p] = [L : K] \cdot a$, d'où $a \mid b$.
Le prochain corollaire montre déjà que la multiplicativité du degré est très utile.

Corollaire 7.15. *Soient $K \subseteq L \subseteq M$ des extensions de corps. Si $[M : K]$ est un nombre premier, alors $L = K$ ou $L = M$.*

Démonstration. Les degrés $[M : L]$ et $[L : K]$ sont des diviseurs du nombre premier $p = [M : K]$, donc, 1 ou p. □

Définition 7.16. *Soient L/K une extension de corps et $a \in L$. Alors, l'application* évaluation *de la proposition 3.9*

$$\mathrm{ev}_a : K[X] \to L, \quad \sum_{i=0}^{d} c_i X^i \mapsto \sum_{i=0}^{d} c_i a^i$$

est un homomorphisme d'anneaux. Pour être plus compact, on écrira aussi $K[X] \ni f(X) \mapsto f(a) \in L$.
*On note l'image de ev_a par $K[a]$ et on l'appelle la K-*algèbre engendrée par *a.*

En tant qu'image de homomorphisme d'anneaux, $K[a]$ est un anneau. Explicitement, $K[a]$ est l'ensemble des éléments dans L qui s'écrivent comme une combinaison K-linéaire des puissances de a :

$$K[a] = \{\sum_{i=0}^{n} c_i a^i \mid n \in \mathbb{N}, c_0, \ldots, c_n \in K\}.$$

Cette forme rend évident le fait que les sommes, les différences et les produits de tels éléments sont aussi de cette forme ; ceci donne une autre preuve que $K[a]$ est un sous-anneau de L. En plus, $K[a]$ est également un K-sous-espace vectoriel de L.
On rappelle qu'une K-algèbre A est un anneau qui est aussi un K-espace vectoriel tel que l'application $K \to A$ donnée par $x \mapsto x.1$ (où $x.1$ est la multiplication scalaire du K-espace vectoriel A) est un homomorphisme d'anneaux. Il est donc évident que $K[a]$ est en effet une K-algèbre.

Remarque 7.17. *Parfois on regardera aussi la variante évidente de la définition 7.16 pour un ensemble (fini ou infini) d'éléments :*
Soient $a_i \in L$ pour $i \in I$ (n'importe quel ensemble). Alors, l'application évaluation

$$\mathrm{ev}_{(a_i)_{i\in I}} : K[X_i \mid i \in I] \to L, \quad f((X_i)_{i\in I}) \mapsto f((a_i)_{i\in I})$$

est un homomorphisme d'anneaux.
*On note l'image de $\mathrm{ev}_{(a_i)_{i\in I}}$ par $K[(a_i)_{i\in I}]$ et on l'appelle la K-*algèbre engendrée par les a_i pour *$i \in I$. Si $I = \{1, 2, 3, \ldots, n\}$ est un ensemble fini, alors on écrit aussi $K[a_1, \ldots, a_n]$.*

Exemple 7.18. *(a) $\mathbb{Q}[2] \subset \mathbb{R}$ est égal à $\mathbb{Q}$.*

(b) Nous avons déjà vu $\mathbb{Q}[i]$ dans l'exemple 3.10, et nous avons vu que $\mathbb{Q}[i]$ est un corps.

(c) L'anneau $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ est égal à $\{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$ parce que

$$\sum_{i=0}^{n} r_i \sqrt{2}^i = \sum_{i=0 \text{ pair}}^{n} r_i 2^{i/2} + (\sum_{i=1 \text{ impair}}^{n} r_i 2^{(i-1)/2})\sqrt{2}.$$

On voit que $\mathbb{Q}[\sqrt{2}]$ est un corps. L'inverse de $a + b\sqrt{2} \neq 0$ est $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Noter que le dénominateur n'est jamais 0, car, s'il l'était, alors $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$. Pour voir que $\sqrt{2} \notin \mathbb{Q}$ il est possible d'utiliser le critère d'Eisenstein.

(d) Soient $n, m \in \mathbb{N}$, $n \neq 0$. On a

$$\mathbb{Q}[\sqrt[n]{m}] = \{\sum_{i=0}^{n-1} a_i \sqrt[n]{m^i} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}.$$

Plus loin, on verra que c'est un corps. Il est aussi possible de démontrer cela « à la main », mais on ne le fera pas.

(e) Soit $n \in \mathbb{N}$, $n > 0$. Posons $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. On appelle ζ_n une racine n-ième primitive de l'unité *car $(\zeta_n)^n = 1$ est $(\zeta_n)^m \neq 1$ pour $0 < m < n$. On trouve (pour n premier)*

$$\mathbb{Q}[\zeta_n] = \{\sum_{i=0}^{n-1} a_i \zeta_n^i \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}.$$

Plus loin, on verra que c'est un corps. Il s'appelle n-ième corps cyclotomique *(en anglais :* cyclotomic field*; en allemand :* Kreisteilungskörper*).*

(f) Soit π le nombre réel appelé π, donc, le nombre réel qui est égal au quotient de la circonférence d'un cercle par son diamétre ou deux fois la valeur du zéro minimal positif de la fonction cos*. Un théorème célèbre de Lindemann (qui n'est pas très difficile, mais, on ne le démontrera pas ; une preuve se trouve par exemple dans le livre de Stewart sur la théorie de Galois) implique (par un argument donné plus loin) que le sous-anneau $\mathbb{Q}[\pi] \subsetneq \mathbb{R}$ n'est pas un sous-corps.*

On donne maintenant la définition du sous-*corps* engendré par un élément. En général, cela n'est pas la même chose que la sous-*algèbre* engendrée par le même élément (sauf si l'élément est algébrique, comme on le verra) à cause de l'existence possible d'éléments non-inversibles.

Définition 7.19. *Soient L/K une extension de corps et $a \in L$. En tant que sous-anneau d'un corps, $K[a]$ est un anneau intègre.*
On définit $K(a)$ comme $\mathrm{Frac}(K[a])$ *et on l'appelle* le sous-corps de L engendré par a sur K *ou bien* l'extension simple de K par a*.*

C'est le plus petit sous-corps de L qui contient K et a car $K[a]$ est le plus petit sous-anneau de L qui contient K et a.

Lemme 7.20. *(a) L'intersection d'un ensemble de sous-corps d'un corps L est un corps lui-même.*

[Attention : l'assertion similaire pour les unions n'est pas vraie.]

(b) $K(a)$ est l'intersection de tous les sous-corps de L qui contiennent K et a.

Démonstration. (a) Clair.
(b) Tout sous-corps de L qui contient K et a, contient $K[a]$ et donc $K(a)$. Donc l'intersection contient $K(a)$. Mais comme $K(a)$ est un des corps utilisés dans l'intersection, on a l'égalité. □

Remarque 7.21. *Parfois on utilisera la définition précédente pour plus qu'un élément :*
Si $a_i \in L$ pour $i \in I$ on définit $K(a_i \mid i \in I)$ comme $\mathrm{Frac}(K[a_i \mid i \in I])$*. C'est l'intersection de tous les sous-corps de L qui contiennent K et les a_i pour $i \in I$. Il est appelé* le sous-corps de L engendré par les a_i pour $i \in I$ sur K.

On jette un deuxième regard sur l'exemple précédent.

Exemple 7.22. *Les exemples suivants seront justifiés dans la prochaine section.*

(a) $\mathbb{Q}[2] = \mathbb{Q}(2) = \mathbb{Q} \subset \mathbb{R}$.

(b) $\mathbb{Q}[i] = \mathbb{Q}(i)$.

(c) $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$.

(d) Soient $n, m \in \mathbb{N}$, $n \neq 0$. *On a* $\mathbb{Q}[\sqrt[n]{m}] = \mathbb{Q}(\sqrt[n]{m})$.

(e) Soit $n \in \mathbb{N}$, $n > 0$. *Posons* $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. *On a* $\mathbb{Q}[\zeta_n] = \mathbb{Q}(\zeta_n)$.

(f) $\mathbb{Q}[\pi] \subsetneq \mathbb{Q}(\pi) \subsetneq \mathbb{R}$. *Remarquons que* $\mathbb{Q}(\pi)$ *est dénombrable, mais* $\mathbb{R}$ *ne l'est pas.*

8 Extensions algébriques

Objectifs :

- Maîtriser la définition d'éléments algébriques et transcendants,
- maîtriser le polynôme minimal d'un élément algébrique,
- connaître la définition et la construction des corps de rupture,
- connaître la définition des extensions algébriques,
- savoir appliquer les propositions importantes,
- connaître des exemples et savoir démontrer des propriétés simples.

Soient L/K une extension de corps et $a \in L$. On traite maintenant la question si la dimension de $K[a]$ en tant que K-espace vectoriel est finie ou infinie. L'idée simple mais importante est de considérer les deux alternatives :

(1) Les éléments $1 = a^0, a, a^2, a^3, a^4, \ldots$ sont K-linéairement indépendants.

(2) Les éléments $1 = a^0, a, a^2, a^3, a^4, \ldots$ sont K-linéairement dépendants.

En cas (1) $K[a]$ est un espace vectoriel de dimension infinie.
En cas (2) il existe une combinaison linéaire

$$0 = \sum_{i=0}^{n} r_i a^i$$

avec $n \in \mathbb{N}$, $r_i \in K$ pour $0 \leq i \leq n$ et $r_n \neq 0$. En divisant par r_n, nous pouvons supposer que cette combinaison linéaire est de la forme

$$0 = a^n + \sum_{i=0}^{n-1} r_i a^i.$$

On peut interpreter cette égalité comme suit : Le polynôme unitaire

$$f(X) := X^n + r_{n-1}X^{n-1} + \cdots + r_1X + r_0 \in K[X]$$

possède a comme zéro : $f(a) = 0$. Dans les propositions suivantes nous allons voir que $K[a]$ est de dimension finie en tant que K-espace vectoriel et que même $K[a]$ est un corps lui-même, donc $K[a] = K(a)$ et $K(a)/K$ est une extension finie de corps.

Définition 8.1. *Soit L/K une extension de corps.*
On appelle algébrique sur K *tout élément $a \in L$ tel qu'il existe un polynôme non-zéro $f \in K[X]$ tel que $f(a) = 0$ (c'est à dire que a est un zéro (ou racine) de f).*
Un élément $a \in L$ qui n'est pas algébrique sur K est appelé transcendant sur K.

Il est important de noter que l'algébricité est une notion *relative*. Un élément est algébrique *sur* un corps (et non algébrique tout seul).

Exemple 8.2. *(a) Soit K un corps. Tout $a \in K$ est algébrique sur K. En effet, a est un zéro du polynôme $X - a \in K[X]$ qui est clairement le polynôme minimal de a sur K.*

(b) $\sqrt{2}$ est algébrique sur $\mathbb{Q}$. En effet, $\sqrt{2}$ est un zéro du polynôme $X^2 - 2 \in \mathbb{Q}[X]$. Ce polynôme est irréductible (par exemple par le critère d'Eisenstein pour $p = 2$). Noter que le polynôme $X - \sqrt{2}$ ne peut pas être utilisé ici car ses coefficients ne sont pas dans $\mathbb{Q}$!

(c) Soit p un nombre premier et $n \in \mathbb{N}$, $n > 1$. Alors, $X^n - p$ est irréductible (critère d'Eisenstein) est possède $\sqrt[n]{p}$ comme zéro, montrant l'algébricité de $\sqrt[n]{p}$ sur $\mathbb{Q}$.

(d) Soit p un nombre premier. On pose $\zeta_p = e^{2\pi i/p}$. Comme $\zeta_p^p = 1$, ζ_p est un zéro du polynôme $X^p - 1 \in \mathbb{Q}[X]$. Donc ζ_p est algébrique sur $\mathbb{Q}$.

(e) π est transcendant sur $\mathbb{Q}$. Ceci est le théorème de Lindemann déjà mentionné. Plus loin, on obtiendra de ce théorème par la théorie de Galois que la quadrature du cercle à la règle et au compas est impossible. Ceci veut dire qu'il est impossible de construire un carré du même aire qu'un cercle donné en utilisant seulement une règle (sans échelle) et un compas.

(f) π est algébrique sur $\mathbb{R}$ (cas spécial de (a)).

(g) $i = \sqrt{-1} \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ car c'est un zéro du polynôme $X^2 + 1 \in \mathbb{Q}[X]$.

Proposition 8.3. *Soient L/K une extension de corps et $a \in L$. Considérons l'évaluation $\mathrm{ev}_a : K[X] \to L$ donnée par $f \mapsto f(a)$ (voir la définition 7.16). Alors*

$$\mathrm{ev}_a \text{ est injectif } \Leftrightarrow a \text{ est transcendant sur } K.$$

Démonstration. Si a est algébrique sur K, alors il existe un polynôme $0 \neq f \in K[X]$ tel que $f(a) = 0$. Alors f est dans le noyau de l'évaluation, donc, ev_a n'est pas injectif. Réciproquement, si ev_a n'est pas injectif, alors il existe un polynôme $f \neq 0$ dans le noyau de ev_a. Ceci ne dit autre que $f(a) = 0$; donc a est algébrique. □

Proposition 8.4. *Soient L/K une extension de corps et $a \in L$ algébrique sur K.*

(a) Il existe un unique polynôme unitaire $\mathrm{mipo}_a(X) \in K[X]$ *tel que* $(\mathrm{mipo}_a) = \ker(\mathrm{ev}_a)$. *C'est-à-dire que l'idéal principal* (mipo_a) *est le noyau de l'évaluation.*

Le polynôme mipo_a *est appelé* le polynôme minimal de a sur K.

(b) Le polynôme minimal $\mathrm{mipo}_a \in K[X]$ *de* a *sur* K *est irréductible (en tant qu'élément de* $K[X]$*).*

C'est l'unique polynôme unitaire irréductible dans $K[X]$ *ayant* a *comme zéro.*

C'est aussi le polynôme unitaire dans $K[X]$ *de degré minimal ayant* a *comme zéro. Cela explique son nom.*

(c) L'application induite par le théorème d'isomorphisme $\mathrm{ev}_a : K[X]/(\mathrm{mipo}_a) \to L, \quad f + (\mathrm{mipo}_a) \mapsto f(a)$ *donne l'isomorphisme*

$$K[X]/(\mathrm{mipo}_a) \cong K[a] = K(a).$$

(d) Soit $d = \deg(\mathrm{mipo}_a)$. *Alors,* $K(a)$ *est une extension finie de* K *de degré* $[K(a) : K] = d$. *Une* K*-base de* $K(a)$ *est donnée par* $1, a, a^2, \ldots, a^{d-1}$.

Démonstration. (a) Nous savons que $K[X]$ est un anneau principal. Donc le noyau de ev_a est un idéal principal, donc engendré par un élément f. Puisque ev_a n'est pas injectif (car a est algébrique sur K), f est non-zéro. Le générateur d'un idéal principal est unique à une unité de l'anneau près. Donc, f est unique à multiplication par une unité de K près (car les unités de $K[X]$ sont les mêmes que celles de K). Si f est de la forme $r_d X^d + r_{d-1} X^{d-1} + \cdots + r_0 \in K[X]$ avec $r_d \neq 0$, alors $\mathrm{mipo}_a := \frac{1}{r_d} f = X^d + \frac{r_{d-1}}{r_d} X^{d-1} + \cdots + \frac{r_0}{r_d}$ est l'unique polynôme unitaire recherché.
(b) Soit $f \in K[X]$ un polynôme non-zéro tel que $f(a) = 0$. Alors $f \in \ker(\mathrm{ev}_a) = (\mathrm{mipo}_a)$, donc $\mathrm{mipo}_a \mid f$. En conséquence le degré de mipo_a est plus petit ou égal au degré de f.
Si mipo_a était réductible, on aurait $\mathrm{mipo}_a = fg$ avec $f, g \in K[X]$ tous les deux de degré strictement plus petit que le degré de mipo_a. Mais, $0 = \mathrm{mipo}_a(a) = f(a)g(a)$ donnerait $f(a) = 0$ ou $g(a) = 0$. Les deux contradiraient la minimalité du degré de mipo_a.
Comme tout polynôme dans $\ker(\mathrm{ev}_a)$ est un multiple de mipo_a, aucun autre polynôme unitaire dans le noyau n'est irréductible.
(c) Puisque mipo_a est irréductible, $K[X]/(\mathrm{mipo}_a)$ est un corps car c'est le quotient par un idéal maximal. Par le théorème d'isomorphisme, l'image de ev_a, qui est par définition ègale à $K[a]$, est un corps. Comme $K[a]$ est un corps, il est égal à son corps des fractions $K(a)$ montrant l'égalité.
(d) Ecrivons le polynôme minimal de a sur K comme $\mathrm{mipo}_a(X) = X^d + c_{d-1} X^{d-1} + \cdots + c_0$. On veut démontrer que $1, a, a^2, a^3, \ldots, a^{d-1}$ est une K-base pour $K[a]$.
D'abord il est clair que ces éléments sont K-linéairement indépendants, car s'ils ne l'étaient pas, alors il y'aurait $r_0, \ldots, r_{d-1} \in K$ pas tous zéro tels que $0 = \sum_{i=0}^{d-1} r_i a^i$, donc le polynôme minimal de a aurait degré strictement plus petit que d, une contradiction.
Donc il faut montrer que $1, a, a^2, a^3, \ldots, a^{d-1}$ engendrent $K[a]$ en tant que K-espace vectoriel. Il suffit de représenter a^n, pour tout n, comme combinaison K-linéaire de $1, a, a^2, a^3, \ldots, a^{d-1}$. Pour le faire on utilise le polynôme minimal qui donne

$$a^d = -\big(c_{d-1} a^{d-1} + \cdots + c_0\big).$$

Supposons que la plus grande puissance de a qui apparaît est a^m pour $m \geq d$. Dans ce cas, nous multiplions l'équation par a^{m-d} et obtenons :

$$a^m = -\big(c_{d-1}a^{m-1} + \cdots + c_0 a^{m-d}\big).$$

Donc on peut exprimer a^m comme une combinaison linéaire de puissances moins élévées de a. Ayant fait cela, il reste au pire des puissances a^{m-1}, et on applique le même processus autant de fois jusqu'à ce que seulement des puissances a^n pour $n \leq d-1$ restent. □

Exemple 8.5 (Continuation de l'exemple 8.2)**.** *(a) Pour un corps K et $a \in K$, le polynôme minimal de a sur K est $X - a \in K[X]$.*

(b) Le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 2 \in \mathbb{Q}[X]$ car il est irréductible et $\sqrt{2}$ est un de ses zéros.

(c) Pour p un nombre premier et $n \in \mathbb{N}_{n>1}$, le polynôme minimal de $\sqrt[n]{p}$ sur $\mathbb{Q}$ est $X^n - p$ car il est irréductible et $\sqrt[n]{p}$ est un de ses zéros.

(d) Soient p un nombre premier et $\zeta_p = e^{2\pi i/p}$. Rappelons que $X^p - 1 = (X-1)\Phi_p(X)$ où $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ est le p-ème polynôme cyclotomique. Comme $\zeta_p - 1 \neq 0$, on trouve $\Phi_p(\zeta_p) = 0$. Comme Φ_p est irréductible, c'est le polynôme minimal de ζ_p sur $\mathbb{Q}$.

(e) Le polynôme minimal de $i = \sqrt{-1} \in \mathbb{C}$ sur $\mathbb{Q}$ est $X^2 + 1 \in \mathbb{Q}[X]$.

Exemple 8.6. *Considérons l'exemple $\mathbb{Q}(\zeta_3)$ pour $\zeta_3 = e^{2\pi i/3}$. Le polynôme minimal de ζ_3 sur $\mathbb{Q}$ est $X^2 + X + 1$, donc $\mathbb{Q}(\zeta_3)$ est l'image de $\mathbb{Q}[X]/(X^2 + X + 1)$ dans $\mathbb{C}$. La $\mathbb{Q}$-base la plus facile c'est $1, \zeta_3$. Donc on exprime tout élément de $\mathbb{Q}(\zeta_3)$ comme $a + b\zeta_3$ pour $a, b \in \mathbb{Q}$.*
Soient $\alpha = a_0 + a_1\zeta_3$ et $\beta = b_0 + b_1\zeta_3$ deux tels éléments. Alors

$$\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\zeta_3$$

et

$$\begin{aligned}\alpha \cdot \beta &= (a_0 + a_1\zeta_3)(b_0 + b_1\zeta_3) = a_0b_0 + \zeta_3(a_0b_1 + a_1b_0) + a_1b_1(\zeta_3)^2 \\ &= (a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0 - a_1b_1)\zeta_3,\end{aligned}$$

car $\zeta_3^2 = -\zeta_3 - 1$ à cause de son polynôme minimal.

Définition 8.7. *Soit K un corps et $f \in K[X]$ un polynôme irréductible non-zéro. On appelle* corps de rupture *du polynôme f sur K toute extension L de K telle qu'il existe $a \in L$ qui satisfait $f(a) = 0$ et $L = K(a)$.*

Exemple 8.8. *Soit L/K une extension de corps et $a \in L$ algébrique. Alors, $K(a)$ est un corps de rupture du polynôme minimal de a sur K.*

Proposition 8.9. *Soit K un corps et $f \in K[X]$ un polynôme irréductible non-zéro. Il existe un corps de rupture de f sur K.*

Démonstration. Ecrivons $f(X) = \sum_{i=0}^{d} a_i X^i \in K[X]$. On pose $L := K[X]/(f(X))$ (c'est bien un corps car f est irréductible) et $\alpha := X + (f)$, la classe de X dans L. L'application naturelle $K \to L$ donnée par $b \mapsto b + (f(X))$ est un homomorphisme de corps. Donc on peut voir K de façon naturelle comme sous-corps de L.
Nous démontrons que α est un zéro de f dans L :

$$f(X + (f(X))) = \sum_{i=0}^{d} a_i (X + (f(X)))^i = \sum_{i=0}^{d} a_i X^i + (f(X)) = f(X) + (f(X)) = 0 + (f(X)).$$

Donc on a $f(\alpha) = 0$ dans L.
Nous obtenons que L est un corps de rupture de f sur K. □

Définition 8.10. *Soit L/K une extension de corps.*
On die que L/K est algébrique *(ou, alternativement, que L est une* extension algébrique *de K) si tout $a \in L$ est algébrique sur K.*
Si L/K n'est pas algébrique, alors elle est dite transcendante.

Proposition 8.11. *Toute extension finie de corps L/K est algébrique. Elle peut être engendrée par un nombre fini d'éléments algébriques sur K.*

Démonstration. Soit $a \in L$. Comme $K[a]$ est un sous-espace de L, il est de K-dimension finie. Donc, a est algébrique sur K. Soit $b_1, \ldots, b_n$ une K-base de L ; c'est aussi un système de générateurs de L sur K. Puisque L/K est algébrique, $b_1, \ldots, b_n$ sont algébriques. □

Proposition 8.12. *Soient L/K une extension de corps et $a_1, \ldots, a_n \in L$. Les deux assertions suivantes sont équivalentes :*

(i) Tous les a_i pour $i = 1, \ldots, n$ sont algébriques sur K.

(ii) L'extension $K(a_1, a_2, \ldots, a_n)/K$ est finie.

Démonstration. Exercice. □

Proposition 8.13. *Soient $M/L/K$ des extensions de corps.*

(a) Supposons que L/K est algébrique et $a \in M$ est algébrique sur L. Alors a est algébrique sur K.

(b) (Transitivité de l'algébricité) M/K est algébrique si et seulement si M/L et L/K sont algébriques.

Démonstration. (a) Soit $\mathrm{mipo}_a = \sum_{i=0}^{d} c_i X^i \in L[X]$ le polynôme minimal de a sur L. Ses coefficients $c_i \in L$ sont algébriques sur K. Donc l'extension $N := K(c_0, c_1, \ldots, c_{d-1})$ de K est finie par la proposition 8.12. Car N contient les coefficients d'un polynôme qui annulle a, l'extension $N(a)$ est algébrique sur N, donc le degré $[N(a) : N]$ est fini. Par la multiplicativité du degré, l'extension $N(a)/K$ est aussi finie, donc algébrique. En particulier, a est algébrique sur K.
(b) Une direction est triviale, l'autre est une conséquence de (a). □

On termine cette partie par une définition très importante, mais, qui ne jouera pas de grand rôle dans ce cours.

Définition 8.14. *Soit L/K une extension de corps et $a_1, \ldots, a_n \in L$. On dit que les éléments $a_1, \ldots, a_n$ sont* algébriquement dépendants sur K *si l'évaluation* $\mathrm{ev}_{a_1,\ldots,a_n}$ *n'est pas injective.*
Dans le cas contraire on parle d'éléments algébriquement indépendants sur K.

Exemple 8.15. *(a) (π, π^2) sont algébriquement dépendants sur $\mathbb{Q}$ (considérer : $X_1^2 - X_2$).*

(b) Il n'est pas connu si (e, π) (avec e la base de l'exponentielle naturelle) sont algébriquement indépendants sur $\mathbb{Q}$.

9 Constructions à la règle et au compas

Objectifs :

- Connaître et savoir faire les constructions fondamentales à la règle et au compas,
- connaître la traduction de la constructibilité à la règle et au compas en langage d'algèbre,
- savoir appliquer cette traduction en algèbre pour résoudre des problèmes de non-constructibilité de l'antiquité,
- connaître des exemples et savoir démontrer des propriétés simples.

Nous regardons des constructions en géométrie plane initiées par les grecs anciens. Pour ces constructions nous nous permettons seulement l'utilisation d'une règle (non graduée) et d'un compas. Dans ce qui suit nous allons regarder $\mathbb{C}$ en même temps comme corps algébriquement clos qui contient $\mathbb{Q}$ et comme le plan réel.
Soit $P_0 \subset \mathbb{C}$ un sous-ensemble. Nous considérons les deux opérations suivantes :

Règle Soit $r_1, r_2 \in P_0$ deux points distincts. Tracer la droite passant par r_1 et r_2.

Compas Soit $r_1, r_2, r_3 \in P_0$. Tracer le cercle de centre r_1 et de rayon la distance entre r_2 et r_3. Cas spécial : $r_3 = r_1$: tracer le cercle de centre r_1 passant par r_2.

Définition 9.1. *Soit $P_0 \subseteq \mathbb{C}$ un sous-ensemble. On dit qu'un point $z \in \mathbb{C}$ peut être* contruit à la règle et au compas en un seul pas à partir de P_0 *si*

- *z est le point d'intersection de deux droites distinctes construites selon l'opération* **règle** *en partant de P_0, ou*
- *z est un point d'intersection d'une droite construite selon l'opération* **règle** *et d'un cercle construit selon l'opération* **compas** *en partant de P_0, ou*
- *z est un point d'intersection de deux cercles construits selon l'opération* **compas** *en partant de P_0.*

Pour $n \in \mathbb{N}_{\geq 1}$ soit P_n le sous-ensemble de $\mathbb{C}$ de tous les points qui peuvent être construits à la règle et au compas en un seul pas à partir de P_{n-1}. On pose $\mathcal{X}(P_0) := \bigcup_{n\geq 0} P_n$, c'est le sous-ensemble de $\mathbb{C}$ de tous les points qui peuvent être construits à la règle et au compas en un nombre fini de pas à partir de P_0.

Proposition 9.2. *Les constructions suivantes peuvent être faites à la règle et au compas, c'est-à-dire en utilisant les opérations* **règle** *et* **compas** *:*

(a) Tracer la droite passant par un point z_1 perpendiculaire à la droite passant par z_2, z_3.

(b) Tracer la droite passant par un point z_1 parallèle à la droite passant par z_2, z_3.

(c) Tracer la médiatrice d'un segment donné par z_1 et z_2.

(d) Additionner deux angles : Soient z_1, z_2, z_3 trois points distincts qui décrivent l'angle α entre la droite passant par z_1 et z_2 et la droite passant par z_1 et z_3. Soient également z_4, z_5, z_6 trois points distincts qui décrivent l'angle β entre la droite passant par z_4 et z_5 et la droite passant par z_4 et z_6. Construire une droite passant par z_1 telle que l'angle entre cette droite et celle passant par z_1 et z_2 est égal à $\alpha + \beta$.

(e) Réflexion d'un point z_1 par rapport à la droite passant par z_2 et z_3.

(f) Construction d'un triangle équilatéral à partir du segment donné par les points distincts z_1 et z_2.

(g) Tracer la bisectrice d'un angle : Soient z_1, z_2, z_3 trois points distincts. Construire une droite D passant par z_1 telle que deux fois l'angle entre D et la droite passant par z_1 et z_2 est égal à l'angle entre la droite passant par z_1 et z_2 et celle passant par z_1 et z_3.

Démonstration. Exercice. □

Remarque 9.3. *On peut montrer (exercice) qu'il suffit de demander le cas spécial mentionné dans l'opération* **compas***, c'est-à-dire, en utilisant seulement* **règle** *et le cas spécial de* **compas***, on peut construire le cercle de centre r_1 et de rayon la distance entre r_2 et r_3.*

Corollaire 9.4. *Soit $P_0 \subseteq \mathbb{C}$ tel que $0, 1 \in P_0$ et $z, z_1, z_2 \in \mathcal{X}(P_0)$. Alors :*

(a) $z_1 + z_2 \in \mathcal{X}(P_0)$*;*

(b) $-z \in \mathcal{X}(P_0)$*;*

(c) $\overline{z} \in \mathcal{X}(P_0)$ *(conjugaison complexe);*

(d) $|z| \in \mathcal{X}(P_0)$*;*

(e) $e^{\pi i/3} \in \mathcal{X}(P_0)$*;*

(f) $|z_1| \cdot |z_2| \in \mathcal{X}(P_0)$*;*

(g) $\frac{1}{|z|} \in \mathcal{X}(P_0)$ *pour* $z \neq 0$*;*

(h) $z_1 \cdot z_2 \in \mathcal{X}(P_0)$*;*

(i) $\frac{1}{z} \in \mathcal{X}(P_0)$ *pour* $z \neq 0$*;*

(j) $\pm\sqrt{z} \in \mathcal{X}(P_0)$.

En particulier, $\mathcal{X}(P_0)$ est un corps qui contient $\mathbb{Q}$ et $\overline{P_0} := \{\overline{z} \mid z \in P_0\}$ et satisfait que pour tout $z \in \mathcal{X}(P_0)$ on a $\sqrt{z} \in \mathcal{X}(P_0)$.

Démonstration. Exercice. □

Proposition 9.5. *Soit $P_0 \subseteq \mathbb{C}$ un sous-corps tel que $\overline{P_0} = P_0$ et $i \in P_0$. Si $z \in P_1$, alors $[P_0(z) : P_0] \leq 2$.*

Démonstration. Notons d'abord que si $z = x + iy \in P_0$ (avec $x, y \in \mathbb{R}$), alors $\overline{z} = x - iy \in P_0$ par hypothèse et donc $x = \frac{1}{2}(z + \overline{z}) \in P_0$ et $y = \frac{1}{2i}(z - \overline{z}) \in P_0$. Pour cela nous avons utilisé $i \in P_0$. Donc, les « coordonnées » de tout $z \in P_0$ (c'est-à-dire, la partie réelle et la partie imaginaire) appartiennent à P_0.
La droite passant par $z_1 = x_1 + iy_1 \in P_0$ et $z_2 = x_2 + iy_2 \in P_0$ est donnée par l'équation

$$0 = (x_2 - x_1)(y - y_1) - (y_2 - y_1)(x - x_1)$$

pour $z = x + iy$. Le cercle de centre $z_3 = x_3 + iy_3 \in P_0$ de rayon $r \in P_0$ est donné par l'équation

$$0 = (x - x_3)^2 + (y - y_3)^2 - r^2.$$

L'intersection de deux telles droites mène donc à un système de deux équations linéaires, d'où ses solutions x, y appartiennent à P_0. Donc $z \in P_0$.
Pour obtenir l'intersection de la droite et du cercle, on peut exprimer y comme une fonction linéaire de x à coefficients dans P_0 (si $x_2 \neq x_1$; sinon, on échange les rôles de x et y) et substituer y dans l'équation du cercle. Cela montre que x satisfait à une équation quadratique à coefficients dans P_0. Cela montre que z appartient à une extension quadratique de P_0.
Finalement, on intersecte le cercle ci-dessus avec le cercle

$$0 = (x - x_4)^2 + (y - y_4)^2 - s^2$$

pour $z_4 = x_4 + iy_4 \in P_0$ et $s \in P_0$. Soit $x + iy$ dans l'intersection. On calcule ainsi :

$$\begin{aligned} 0 &= ((x - x_3) + (x_3 - x_4))^2 + ((y - y_3) + (y_3 - y_4))^2 - s^2 \\ &= (x - x_3)^2 + (y - y_3)^2 + 2(x - x_3)(x_3 - x_4) + 2(y - y_3)(y_3 - y_4) + (x_3 - x_4)^2 + (y_3 - y_4)^2 - s^2 \\ &= 2(x - x_3)(x_3 - x_4) + 2(y - y_3)(y_3 - y_4) + (x_3 - x_4)^2 + (y_3 - y_4)^2 + r^2 - s^2 = 0. \end{aligned}$$

Les points d'intersection des deux cercles se trouvent donc sur une droite. Par cette substitution, nous avons donc remplacé l'équation du deuxième cercle par une équation linéaire. Puisque nous avons déjà traité le cas de l'intersection d'un cercle et d'une droite, la démonstration est achevée. □

Lemme 9.6 (Premier cas de la théorie de Kummer)**.** *Soit L/K une extensions de corps de caractéristique différent de 2 tel que $[L : K] = 2$. Alors il existe $a \in K$ tel que $L = K(\sqrt{a})$.*

Démonstration. Soit $b \in L \setminus K$ et $X^2 + rX + s \in K[X]$ le polynôme minimal de b sur K. Posons $a := b + \frac{r}{2} \in L \setminus K$. Alors :

$$a^2 = b^2 + br + \frac{r^2}{4} = \frac{r^2}{4} - s \in K.$$

Donc le polynôme minimal de a est $X^2 - \frac{r^2}{4} + s \in K[X]$ et $L = K(b) = K(a) = K(\sqrt{\frac{r^2}{4} - s})$. □

On appliquera le lemme ainsi : Si K est un corps contenu dans $\mathcal{X}(P_0)$ et L/K est une extension de degré 2, alors L est aussi contenu dans $\mathcal{X}(P_0)$. Cela peut être itéré pour des extensions successives de degré 2. C'est la clé dans le théorème suivant.

Théorème 9.7. *Soit $P_0 \subseteq \mathbb{C}$ avec $0, 1 \in P_0$. Posons $L_0 := \mathbb{Q}(P_0 \cup \overline{P_0})$. On a $L_0 \subseteq \mathcal{X}(P_0)$ à cause du corollaire 9.4. Soit $z \in \mathbb{C}$. Les deux assertions suivantes sont équivalentes :*

(i) $z \in \mathcal{X}(P_0)$.

(ii) Il existe $n \in \mathbb{N}$ et pour tout $1 \leq j \leq n$ un corps L_j tel que

$$L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_n$$

et $z \in L_n$ et pour tout $1 \leq j \leq n$ on a $[L_j : L_{j-1}] = 2$.

Démonstration. « (i) $\Rightarrow$ (ii) » : On remarque d'abord qu'il suffit de construire une suite de corps comme dans l'énoncé mais avec $L_{j-1} \subseteq L_j$ et $[L_j : L_{j-1}] \leq 2$. Sans perte de généralité nous pouvons supposer $P_0 = \mathbb{Q}(P_0 \cup \overline{P_0}) = L_0$ parce que $\mathcal{X}(P_0) = \mathcal{X}(L_0)$. Comme i peut être construit à partir de $0, 1$ et $[L_0(i) : L_0] \leq 2$, nous pouvons aussi supposer $i \in P_0$. On a $\overline{L_0} = L_0$
Soit $j \in \mathbb{Z}_{\geq 0}$. Si on construit un point w à partir d'un corps $L_j \subseteq \mathbb{C}$ avec $i \in L_j$ et $\overline{L_j} = L_j$ en un seul pas, par la proposition 9.5 on a $[L_j(w) : L_j] \leq 2$ et $[L_j(\overline{w}) : L_j] \leq 2$. On pose $L_{j+1} := L_j(w)$ et $L_{j+2} := L_{j+1}(\overline{w}) = L_j(w, \overline{w})$. Nous avons $[L_{j+2} : L_{j+1}] \leq 2$ et $[L_{j+1} : L_j] \leq 2$ et $L_{j+2} = \overline{L_{j+2}}$. La dernière égalité nous permet d'itérer la procédure.
Pour conclure, il suffit de voir que pour construire $z \in \mathcal{X}(P_0)$, il suffit de faire un nombre fini de constructions à la règle et au compas en un pas. Par définition, il existe $m \in \mathbb{Z}_{\geq 0}$ tel que $z \in P_m$. La construction de z implique un ensemble fini de points (ceux qui définissent la/les droite(s) et le(s) cercle(s) qui sont intersectés) dans P_{m-1}. La construction de chacun de ces points implique un ensemble fini de points dans P_{m-2}, etc. Donc, pour construire z, il suffit de faire un nombre fini de constructions.
« (ii) $\Rightarrow$ (i) » : Le lemme 9.6 nous dit que pour tout $1 \leq j \leq n$, il existe $z_j \in L_{j-1}$ tel que $L_j = L_{j-1}(\sqrt{z_j})$. Par le corollaire 9.4, $\mathcal{X}(P_0)$ est un corps fermé sous les racines carrées, nous obtenons $L_n \subseteq \mathcal{X}(P_0)$, donc $z \in \mathcal{X}(P_0)$. □

Corollaire 9.8. *Soit $P_0 \subseteq \mathbb{C}$ avec $0, 1 \in P_0$.*

(a) L'extension de corps $\mathcal{X}(P_0)/\mathbb{Q}(P_0 \cup \overline{P_0})$ est algébrique.

(b) Pour tout $z \in \mathcal{X}(P_0)$ il existe $r \in \mathbb{N}$ tel que $[\mathbb{Q}(P_0 \cup \overline{P_0} \cup \{z\}) : \mathbb{Q}(P_0 \cup \overline{P_0})] = 2^r$.

Démonstration. C'est une conséquence directe du théorème 9.7 et la multiplicativité des degrés pour (b). □

Théorème 9.9 (Wantzel)**.** *Le cube ne peut pas être dupliqué à la règle et au compas ; c'est-à-dire, si $\overline{AB}$ est un coté d'un cube, il est impossible de construire à la règle et au compas un segment $\overline{CD}$ tel que le volume du cube ayant le coté $\overline{CD}$ est le double du volume du cube ayant le coté $\overline{AB}$.*

Démonstration. Sans perte de généralité nous pouvons prendre $A = 0$ et $B = 1$. Il s'agit donc de construire $\sqrt[3]{2}$. C'est impossible car $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (pas de puissance de 2). □

Théorème 9.10 (Wantzel)**.** *Il est impossible de trisecter un angle donné à la règle et au compas.*

Démonstration. Par exemple on peut regarder l'angle $e^{\pi i/3}$ (dans le triangle éqilatéral avec coté $\overline{01}$). Si on pouvait le trisecter, on aurait construit $e^{\pi i/9}$. Mais son polynôme minimal est $X^6 - X^3 + 1 \in \mathbb{Z}[X]$ (exercice), dont le degré $[\mathbb{Q}(e^{\pi i/9}) : \mathbb{Q}] = 6$ n'est pas une puissance de 2. □

Théorème 9.11. *La quadrature du cercle est impossible ; c'est-à-dire, pour un cercle donné, il est impossible de construire, à la règle et au compas, un carré du même aire que le cercle.*

Démonstration. L'aire du cercle unitaire est π. Si la construction était possible, on aurait construit $\sqrt{\pi}$, et en particulier $\sqrt{\pi}$ serait algébrique sur $\mathbb{Q}$, ce qui n'est pas le cas, comme par le théorème de Lindemann π (et donc aussi $\sqrt{\pi}$) est transcendant sur $\mathbb{Q}$. □

Remarque 9.12. *Un théorème remarquable de Mohr et Mascheroni, démontré indépendamment par Georg Mohr en 1672 et par Lorenzo Mascheroni en 1797, affirme que si une construction géométrique est possible à la règle et au compas, alors elle est possible au compas seul (sauf le tracé effectif des droites).*

10 Corps de décomposition

Objectifs :

- Maîtriser la définition de la clôture algébrique d'un corps dans une extension et ses propriétés fondamentales ;
- maîtriser les prolongations d'homomorphismes de corps,
- en particulier, connaître la relation entre les racines d'un polynôme irréductible et des prolongations de l'identité ;
- connaître la définition et les propriétés fondamentales du corps de décomposition ;
- connaître la définition et les propriétés fondamentales des extensions normales ;
- connaître des exemples et savoir démontrer des propriétés simples.

Clôture algébrique

Définition-Lemme 10.1. *Soit L/K une extension de corps. On pose*

$$K_L := \{a \in L \mid a \text{ algébrique sur } K\}.$$

On appelle K_L la clôture algébrique de K dans L.

(a) $K_L = L \Leftrightarrow L$ est algébrique sur K.

(b) K_L est un sous-corps de L.

(c) K_L/K est une extension algébrique et tout $x \in L \setminus K_L$ est transcendant sur K_L.

Démonstration. (a) par définition.
(b) Soient $a, b \in K_L$. Il est difficile (mais, pas impossible) d'écrire les polynômes minimaux pour $a + b$, $a \cdot b$, et $1/b$ (si $b \neq 0$) en partant des polynômes minimaux de a et b en utilisant le résultant (voir la définition 6.25).
On va le faire autrement : $K(a, b)$ est une extension finie et algébrique de K (comme $a, b \neq 0$ sont algébriques sur K). Donc $a+b, a\cdot b, 1/b \in K(a, b)$ sont algébriques sur K, donc $a+b, a\cdot b, 1/b \in K_L$. Donc, K_L est un sous-corps de L.
(c) L'extension K_L/K est algébrique par sa construction. Si $x \in L \setminus K_L$ était algébrique sur K_L, par la transitivité de l'algébricité (proposition 8.13), x serait aussi algébrique sur K, donc $x \in K_L$, contradiction. □

Exemple 10.2. $\overline{\mathbb{Q}} := \mathbb{Q}_{\mathbb{C}}$ *est la clôture algébrique de* $\mathbb{Q}$ *dans* $\mathbb{C}$*. Il satisfait les propriétés suivantes :*

(a) $\overline{\mathbb{Q}}/\mathbb{Q}$ *est algébrique.*

(b) $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ *(par exemple,* $X^n - p \in \mathbb{Z}[X]$ *est irréductible pour tout* n *et tout nombre premier* p *par le critère d'Eisenstein ; donc* $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$*).*

(c) $\overline{\mathbb{Q}}$ *est dénombrable (car l'ensemble de polynômes dans* $\mathbb{Q}[X]$ *est dénombrable, donc l'ensemble de leurs zéros l'est aussi).*

(d) $\mathbb{C}$ *n'est pas dénombrable. Donc dans* $\mathbb{C}$ *il existe un ensemble non-dénombrable d'éléments qui sont transcendants sur* $\mathbb{Q}$*.*

Définition 10.3. *On appelle* algébriquement clos *tout corps* K *pour lequel tout* $f \in K[X]$ *de degré* ≥ 1 *possède un zéro dans* K*.*
On appelle clôture algébrique d'un corps K *toute extension algébrique* $\overline{K}/K$ *telle que* $\overline{K}$ *est algébriquement clos.*

Exemple 10.4. $\mathbb{C}$ *est algébriquement clos (c'est un résultat d'analyse complexe, par exemple).*
Le corps $\overline{\mathbb{Q}}$ *de l'exemple 10.2 est une clôture algébrique de* $\mathbb{Q}$*.*

Lemme 10.5. *Soit* K *un corps. Les assertions suivantes sont équivalentes :*

(i) K *est algébriquement clos.*

(ii) Tout $f \in K[X]$ *unitaire de degré* d *est de la forme*

$$f(X) = \prod_{i=1}^{d} (X - a_i)$$

avec $a_1, \ldots, a_d \in K$*.*

(iii) Si L/K *est une extension algébrique, alors* $L = K$*.*

Démonstration. « (i) ⇒ (ii) » C'est une application de la division euclidienne de polynômes (voir la proposition 7.9).

« (ii) $\Rightarrow$ (iii) » : Soit L/K algébrique, soit $a \in L$ et soit $f \in K[X]$ le polynôme minimal de a sur K. Tous les zéros de f sont dans K, donc $a \in K$. Donc $L = K$.
« (iii) $\Rightarrow$ (i) » : Soit $f \in K[X]$ un polynôme non-constant. On peut supposer sans perte de généralité qu'il est irréductible. L'extension $L := K[X]/(f)$ sur K est algébrique, donc $L = K$, donc le degré de f est 1, donc f a un zéro dans K. □

Théorème 10.6. *Soit K un corps. Il existe une clôture algébrique de K.*

Démonstration. Exercice. □

Prolongation d'homomorphismes de corps

Dans la suite, les zéros du polynôme minimal d'un éléments vont jouer un rôle crucial. C'est pour cela que nous commençons par le lemme suivant (facile).

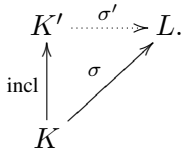
Lemme 10.7. *Soit L/K une extension de corps.*

(a) Soit $f \in K[X]$ irréductible. Soit $b \in L$ est tel que $f(b) = 0$. Alors $\mathrm{mipo}_b = f$.

(b) Soit $a \in L$ algébrique sur K et $b \in L$ tel que $\mathrm{mipo}_a(b) = 0$. Alors, $\mathrm{mipo}_b = \mathrm{mipo}_a$.

Démonstration. (a) provient directement de la proposition 8.4 et (b) suit de (a). □

Définition 10.8. *Soient K'/K une extension de corps, L un corps et $\sigma : K \to L$ et $\sigma' : K' \to L$ des homomorphismes de corps.*
On dit que σ' est une prolongation de σ *si $\sigma'|_K = \sigma$ (c'est-à-dire, $\sigma'(x) = \sigma(x)$ pour tout $x \in K$).*
On visualise la situation par le diagramme



Notation 10.9. *Soient K, L des corps et $\sigma : K \to L$ un homomorphisme de corps. Pour un polynôme $f(X) = \sum_{i=0}^{d} a_i X^i \in K[X]$ nous écrivons f^σ pour le polynôme $\sum_{i=0}^{d} \sigma(a_i) X^i \in L[X]$.*

Lemme 10.10. *Soient K, L des corps, $K' = K(a)$ une extension algébrique de K et $f := \mathrm{mipo}_a \in K[X]$. Soit $\sigma : K \to L$ un homomorphisme de corps. Alors :*

(a) Si $\sigma' : K' \to L$ est une prolongation de σ (c'est-à-dire, un homomorphisme de corps tel que $\sigma'|_K = \sigma$), alors $f^\sigma(\sigma'(a)) = 0$, donc $\sigma'(a)$ est un zéro de f^σ.

En particulier, si $f^\sigma = f$, alors σ' permute les racines de f.

(b) Pour tout zéro $b \in L$ de f^σ il existe une unique prolongation $\sigma' : K' \to L$ telle que $\sigma'(a) = b$.

En particulier, si $K \subseteq L$ and σ est égal à l'inclusion, alors pour toute racine $b \in L$ de f, il existe un unique homomorphisme $\sigma' : K' \to L$ qui envoie a sur b et est égal à l'identité sur K.

(c) Le nombre de prolongations de σ à K' est égal au nombre de zéros de f^σ dans L, donc au plus égal à $\deg(f)$.

Démonstration. (a) Soit $f(X) = \sum_{i=0}^d c_i X^i$. On a

$$f^\sigma(\sigma'(a)) = \sum_{i=0}^d \sigma(c_i)\sigma'(a)^i = \sum_{i=0}^d \sigma'(c_i)\sigma'(a)^i = \sigma'\left(\sum_{i=0}^d c_i a^i\right) = \sigma'\left(f(a)\right) = \sigma'(0) = 0.$$

(b)

Unicité Comme K' a la K-base $1, a, a^2, \ldots, a^{d-1}$, toute prolongation $\sigma' : K' \to L$ de σ est uniquement déterminée par l'image de a car $\sigma'(\sum_{i=0}^d r_i a^i) = \sum_{i=0}^d \sigma(r_i)\sigma'(a)^i$.

Existence Considérons l'homomorphisme d'anneaux

$$\phi : K[X] \xrightarrow{h \mapsto h^\sigma} L[X] \xrightarrow{\mathrm{ev}_b,\ g \mapsto g(b)} L.$$

On a clairement $\phi|_K = \sigma$ (ici K est identifié avec les polynômes constants dans $K[X]$). On a aussi $f \in \ker(\phi)$ car $f^\sigma(b) = 0$. Comme f est irréductible, l'idéal $(f) \lhd K[X]$ est maximal, donc $(f) = \ker(\phi)$. Le théorème d'isomorphisme fournit un homomorphisme d'anneaux

$$\overline{\phi} : K[X]/(f(X)) \to L,$$

qui est injectif et satisfait $\overline{\phi}(X + (f)) = b$ et $\overline{\phi}|_K = \sigma$.

Rappelons que $\overline{\mathrm{ev}_a} : K[X]/(f) \to K'$ est un isomorphisme de corps. Donc, $\sigma' := \overline{\phi} \circ \overline{\mathrm{ev}_a}^{-1}$ est la prolongation de σ recherchée.

(c) est une conséquence directe de (a) et (b). □

Exemple 10.11. *(a) On veut étendre l'identité $\mathbb{Q} \hookrightarrow \mathbb{C}$ à $K' := \mathbb{Q}(\sqrt{2})$. Un homomorphisme $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$ est uniquement déterminé par l'image de $\sqrt{2}$. Nous avons donc deux possibilités pour cette image, car elle doit être un zéro du polynôme $f^\sigma(X)$ pour $f(X) = X^2 - 2$. Mais $f^\sigma = f$, donc, soit l'image et $\sqrt{2}$, soit $-\sqrt{2}$.*

(b) On veut étendre l'identité $\mathbb{Q} \hookrightarrow \mathbb{C}$ à $K' := \mathbb{Q}(\sqrt[3]{2})$. De la même manière nous trouvons que l'image de $\sqrt[3]{2}$ doit être une racine de $X^3 - 2$. Pour cette raison nous le factorisons dans $\mathbb{C}$:

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta_3\sqrt[3]{2})(X - \zeta_3^2\sqrt[3]{2})$$

avec $\zeta_3 = e^{2\pi/3}$. Donc, nous avons trois prolongations possibles, à savoir, l'image de $\sqrt[3]{2}$ est soit $\sqrt[3]{2}$, soit $\zeta_3\sqrt[3]{2}$, soit $\zeta_3^2\sqrt[3]{2}$.

Proposition 10.12. *Soient K'/K une extension algébrique (qui peut être infinie), L un corps algébriquement clos et $\sigma : K \to L$ un homomorphisme de corps. Alors :*

(a) Il existe une prolongation $\sigma' : K' \to L$ de σ.

(b) Si K' est algébriquement clos et $L/\sigma(K)$ est algébrique, alors toute prolongation $\sigma' : K' \to L$ de σ est un isomorphisme de corps.

Démonstration. (a) Cet argument utilise le lemme de Zorn 4.24. Regardons l'ensemble

$$M := \{(F, \tau) \mid K'/F/K \text{ extensions de corps, } \tau : F \to L \text{ prolongation de } \sigma\}.$$

- $M \neq \emptyset$ car $(K, \sigma) \in M$.
- M est (partiellement) ordonné pour la relation d'ordre définie par

$$(F_1, \tau_1) \leq (F_2, \tau_2) \Leftrightarrow F_1 \subseteq F_2 \text{ et } \tau_2|_{F_1} = \tau_1.$$

- Tout sous-ensemble $T \subseteq M$ qui est totalement ordonné (c'est-à-dire, pour tout $(F_1, \tau_1) \in T$, $(F_2, \tau_2) \in T$ on a $(F_1, \tau_1) \leq (F_2, \tau_2)$ ou $(F_2, \tau_2) \leq (F_1, \tau_1)$) possède une majorante dans M, à savoir $(\tilde{f}, \tilde{\tau})$ avec $\tilde{F} = \bigcup_{(F,\tau)\in M} F$ et $\tilde{\tau} : F \to L$ défini par $\tilde{\tau}(x) := \tau(x)$ pour un (n'importe lequel) $(F, \tau) \in M$ tel que $x \in F$.

Nous avons vérifié les hypothèses du lemme de Zorn qui nous donne donc un élément maximal $(F, \tau) \in M$. Nous montrons $F = K'$. Si cela n'était pas le cas, alors on pourrait choisir $a \in K' \setminus F$. Comme K'/K est algébrique, a l'est aussi. Donc, par le lemme 10.10 on peut prolonger τ à $F(a)$, c'est une contradiction à la maximalité.
(b) On choisit une prolongation $\sigma' : K' \to L$ (possible par (a)). Comme σ' est injectif (comme tout homomorphisme de corps), K' est isomorphe à $\sigma'(K')$. Donc, $\sigma'(K')$ est aussi algébriquement clos. Par hypothèse, $L/\sigma(K)$ est algébrique, donc $L/\sigma'(K')$ est aussi algébrique, et en conséquence $L = \sigma'(K')$. Donc, σ' est un isomorphisme de corps. □

Définition 10.13. *Soit K un corps. On appelle K-*homomorphisme *tout homomorphisme de corps $\sigma : L_1 \to L_2$ pour des extensions de corps L_1/K et L_2/K tel que σ prolonge* $\mathrm{id} : K \to L_2$ *(c'est-à-dire, si $\sigma(x) = x$ pour tout $x \in K$).*
L'ensemble de tous les K-homomorphismes de L_1 dans L_2 est noté $\mathrm{Hom}_K(L_1, L_2)$.

Exemple 10.14. *Soient $K/\mathbb{Q}$ et $L/\mathbb{Q}$ deux extensions et $\sigma : K \to L$ un homomorphisme de corps. Alors, σ est un $\mathbb{Q}$-homomorphisme.*

Corollaire 10.15. *Soit K un corps et $\overline{K}_1$ et $\overline{K}_2$ deux clôtures algébriques de K. Alors, il existe un isomorphisme de corps $\overline{K}_1 \to \overline{K}_2$ qui prolonge* id_K.

Démonstration. On prolonge l'identité $\mathrm{id} : K \to \overline{K}_2$ à $\overline{K}_1$ par la proposition 10.12 et on trouve un isomorphisme. □

Corps de décomposition

Définition 10.16. *Soient K un corps et $(f_i)_{i\in I} \subseteq K[X]$ une famille de polynômes de degré ≥ 1. On appelle* corps de décomposition de $(f_i)_{i\in I}$ sur K *toute extension L/K telle que*

- *pour tout $i \in I$ le polynôme f_i se factorise complètement en facteurs linéaires dans $L[X]$ ($f_i(X) = b_i \prod_{j=1}^{\deg(f_i)} (X - c_{i,j})$ pour $b, c_{i,j} \in L$) et*
- *L est engendré sur K par tous les $c_{i,j}$ ($L = K(c_{i,j} \mid i \in I, 1 \leq j \leq \deg(f_i))$).*

Souvent la famille de polynômes ne consistera que d'un seul polynôme.

Exemple 10.17. *(a) Le corps de décomposition de $X^2 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt{2})$.*

(b) Le corps de décomposition de $X^3 - 2 \in \mathbb{Q}[X]$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ avec $\zeta_3 = e^{2\pi i/3}$.

(c) Le corps de décomposition de $\{X^2 - 2, X^2 - 3\} \subset \mathbb{Q}[X]$ est $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Proposition 10.18. *Soient K un corps et $(f_i)_{i\in I} \subseteq K[X]$ une famille de polynômes de degré ≥ 1.*

(a) Il existe un corps de décomposition L de la famille $(f_i)_{i\in I}$ sur K. Il est algébrique sur K.

En particulier, si $\tilde{K}$ est une extension algébrique de K qui contient toutes les racines (par exemple, si $\tilde{K}$ est une clôture algébrique de K), le sous-corps de $\tilde{K}$ engendré sur K par toutes les racines dans $\tilde{K}$ de tous les f_i pour $i \in I$ est un corps de décomposition de la famille $(f_i)_{i\in I}$ sur K.

(b) Si L_1 est L_2 sont deux corps de décomposition de cette famille, alors il existe un K-isomorphisme $\sigma : L_1 \to L_2$.

Démonstration. (a) Soit $\overline{K}$ une clôture algébrique de K et soient $c_{i,j} \in \overline{K}$ les zéros des polynômes f_i. Alors, $L := K(c_{i,j} \mid i \in I, 1 \leq j \leq \deg(f_i))$ est un corps de décomposition. Comme L est engendré par des éléments qui sont algébriques sur K, il suit que L/K est une extension algébrique.
(b) Soit $\overline{L}_2$ une clôture algébrique de L_2 et $\mathrm{id}_K : K \to \overline{L}_2$ l'identité. Par la proposition 10.12 on peut prolonger id_K en un K-homomorphisme $\sigma : L_1 \to \overline{L}_2$. On pose $d_{i,j} := \sigma(c_{i,j}) \in \overline{L}_2$. On a

$$b_i \prod_{j=1}^{\deg(f_i)} (X - c_{i,j}) = f_i(X) = f_i^\sigma(X) = b_i \prod_{j=1}^{\deg(f_i)} (X - d_{i,j})$$

et, comme L_2 est engendré sur K par les $d_{i,j}$ en tant que corps de décomposition sur K, alors, l'image $\sigma(L_1)$ est L_2, donc $L_1 \cong L_2$ par le K-isomorphisme σ. □

Définition 10.19. *On appelle* normale *toute extension algébrique de corps L/K telle que tout polynôme irréductible $f \in K[X]$ qui possède un zéro c_1 dans L se factorise complètement en facteurs linéaires dans $L[X]$, c'est-à-dire, $f(X) = b\prod_{i=1}^{\deg(f)}(X - c_i)$ avec $c_1, \ldots, c_{\deg(f)} \in L$.*

Proposition 10.20. *Soit L/K une extension algébrique (pas nécéssairement finie). Alors les assertions suivantes sont équivalentes :*

(i) L/K est normal.

(ii) L est un corps de décomposition d'une famille $(f_i)_{i\in I} \subseteq K[X]$ sur K.

(iii) Tout K-homomorphisme $\sigma : L \to \overline{L}$, où $\overline{L}$ est une clôture algébrique de L, satisfait $\sigma(L) = L$ et donc donne lieu à un K-isomorphisme $\sigma : L \to L$.

Démonstration. « (i) $\Rightarrow$ (ii) » : Soit $S \subseteq L$ tel que $L = K(S)$. Pour tout $s \in S$ soit $f_s := \mathrm{mipo}_s(X) \in K[X]$ le polynôme minimal de s sur K. Par (i), tout f_s se factorise complètement dans $L[X]$, donc toutes les racines appartiennent à L. Par hypothèse L est engendré par $s \in S$, donc, par tous les zéros de tous les f_s. Nous avons donc que les inclusions

$$L = K(S) = K(\text{toutes les racines de tout } f_s, s \in S) \subseteq L$$

sont des égalités.
« (ii) $\Rightarrow$ (iii) » : Nous savons $L = K(c_{i,j} : i \in I, 1 \leq j \leq e_i)$ où pour $i \in I$, les $c_{i,j} \in L$ pour $1 \leq j \leq e_i$ sont les racines de f_i. Donc,

$$\sigma(L) = K(\sigma(c_{i,j}) : i \in I, 1 \leq j \leq e_i) = K(c_{i,j} : i \in I, 1 \leq j \leq e_i) = L.$$

L'égalité du milieu provient du lemme 10.10(a) : pour tout $i \in I$, l'homomorphisme σ permute les $c_{i,j}$.
« (iii) $\Rightarrow$ (i) » : Soient $f \in K[X]$ irréductible et $a \in L$ tel que $f(a) = 0$. Soient $\overline{L}$ une clôture algébrique de L et $b \in \overline{L}$ tel que $f(b) = 0$. Par le lemme 10.10 (b) il existe un K-homomorphisme $\sigma : K(a) \to \overline{L}$ tel que $\sigma(a) = b$. Par la proposition 10.12 on peut le prolonger en K-homomorphisme $\sigma : L \to \overline{L}$. Par (iii) nous avons $L = \sigma(L) \ni \sigma(a) = b$. Donc L contient toutes les racines de f. □

Exemple 10.21. *(a) Les corps $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ et $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sont normaux sur $\mathbb{Q}$.*

(b) Le corps $K := \mathbb{Q}(\sqrt[3]{2})$ n'est pas normal sur $\mathbb{Q}$, car le polynôme $X^3 - 2$ n'a qu'une seule de ses racines dans K. Alternativement, l'image de l'homomorphisme $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ donné par $\sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2}$ n'est pas contenue dans $\mathbb{Q}(\sqrt[3]{2})$.

(c) Toute extension L/K de degré 2 est normale : Si $L = K(a)$, alors L est le corps de décomposition du polynôme minimal de a sur K (comme le polynôme est de degré 2, s'il a un facteur linéaire dans $L[X]$, alors l'autre doit y être aussi).

(d) Bien que M/L et L/K soient normaux, l'extension M/K peut être non-normale.

Par exemple, $\mathbb{Q}(\sqrt[4]{2}) \supsetneq \mathbb{Q}(\sqrt{2}) \supsetneq \mathbb{Q}$. La grande extension n'est pas normale pour les mêmes raison que dans le deuxième exemple. Par contre, les deux sous-extensions sont normales car elles sont de degrés 2.

(e) Si $M/L/K$ sont des extensions de corps avec M/K normal, l'extension L/K peut être non-normale.

Par exemple : $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) \supsetneq \mathbb{Q}(\sqrt[3]{2}) \supsetneq \mathbb{Q}$.

(f) Soient K un corps et $\overline{K}$ une clôture algébrique de K. Alors, $\overline{K}/K$ est normal (on peut prendre la famille de tous les polynômes de $K[X]$).

Proposition 10.22. *Soient $M/L/K$ des extensions de corps. Si M/K est normal, alors M/L l'est aussi.*

Démonstration. Par hypothèse, M est le corps de décomposition d'une famille $(f_i)_{i \in I} \subseteq K[X]$ de polynômes sur K. Mais, M est encore un corps de décomposition de la même famille considérée sur L. □

Définition 10.23. *On appelle* clôture normale d'une extension algébrique L/K *toute extension* N/L *telle que*

- N/K *est normal et*
- *si* $N/N_1/L$ *est tel que* N_1/K *est normal, alors* $N = N_1$ *(donc,* N/K *ne contient aucune sous-extension non-triviale qui est normale sur* K *et contient* L*).*

Proposition 10.24. *Soit* L/K *une extension algébrique.*

(a) Soient $\overline{L}$ *une clôture algébrique de* L *sur* K*,* $S \subseteq L$ *tel que* $L = K(S)$ *et* f_s *le polynôme minimal de* s *sur* K *pour tout* $s \in S$*. Alors, tout corps de décomposition* M *de la famille* $(f_s)_{s\in S}$ *sur* K *est une clôture normale de* L/K*.*

En particulier, une clôture normale existe toujours.

(b) Si N *est une clôture normale de* L/K*, alors* N *est un corps de décomposition sur* K *de la famille* $(f_s)_{s\in S}$ *avec* $L = K(S)$ *comme dans (a).*

(c) Si L/K *est une extension finie, alors toute clôture normale* N/K *de* L/K *est aussi une extension finie.*

(d) Soit N/K *une clôture normale de* L/K*. Alors,* N *est l'extension de* K *engendrée par tous les* $\sigma(L)$ *pour* $\sigma \in \mathrm{Hom}_K(L, \overline{L})$*.*

(e) Si N_1/K *et* N_2/K *sont deux clôtures normales de* L/K*, alors, il existe un* K*-isomorphisme* $N_1 \cong N_2$*.*

Démonstration. (a) Les corps de décomposition donnent lieu à des extensions normales, donc M/K est normale. Soit $M/M'/L$ telle que M'/K est normale. On sait que M' doit contenir toutes les racines des f_s, car $f_s(s) = 0$ et $s \in L$. Donc, $M' = M$.
(b) Soit N une clôture normale de L/K. Comme dans (a) on sait que N doit contenir toutes les racines des f_s, car $f_s(s) = 0$ et $s \in L$. Donc N est un corps de décomposition sur K de la famille $(f_s)_{s\in S}$.
(c) Si L/K est fini, l'ensemble S peut être choisi fini. Donc, on obtient N comme l'extension engendrée par l'ensemble fini de toutes les racines des f_s.
(d) On montre d'abord $N \supseteq \sigma(L)$ pour tout $\sigma \in \mathrm{Hom}_K(L, \overline{L})$: l'image de σ est engendrée par les $\sigma(s)$ pour $s \in S$ (car L est engendré sur K par S). Mais, nous savons que $\sigma(s) \in \overline{L}$ est une racine de f_s et appartient donc à N.
On montre maintenant que N est contenu dans le corps engendré sur K par toutes les images $\sigma(L)$ pour $\sigma \in \mathrm{Hom}_K(L, \overline{L})$. Par (b), pour cela il suffit de démontrer que pour tout $s \in S$ toute racine de f_s est contenue dans un $\sigma(L)$. Soit t une racine de f_s. Nous avons déjà fait cet argument un nombre de fois : par le lemme 10.10 il existe un K-homomorphisme $\sigma : K(s) \to \overline{L}$ qui envoie s sur t. Par la proposition 10.12 nous pouvons prolonger σ en élément de $\mathrm{Hom}_K(L, \overline{L})$. Donc $t \in \sigma(L)$.
(e) Tous les deux sont des corps de décomposition de la famille $(f_s)_{s\in S}$, donc isomorphes par la proposition 10.18 (b). □

11 Extensions séparables

Objectifs :

- Maîtriser la notion de polynôme séparable, en connaître des caractérisations et des exemples ;
- maîtriser les notions d'élément séparable et extension séparable, en connaître des caractérisations et des exemples ;
- connaître et savoir appliquer le degré de séparabilité, en particulier, sa multiplicativité,
- connaître et savoir utiliser l'existence des éléments primitifs dans les extensions séparables finies ;
- maitriser la classification des corps finis ;
- connaître des exemples et savoir démontrer des propriétés simples.

Rappel : Soient K un corps, $f \in K[X]$ un polynôme irréductible, $\overline{K}$ une clôture algébrique de K et $a \in \overline{K}$ t.q. $f(a) = 0$. Alors, nous avons la bijection

$$\{b \in \overline{K} \mid f(b) = 0\} \longrightarrow \mathrm{Hom}_K(K(a), \overline{K}),$$

où l'image de la racine b est l'unique K-homomorphisme σ tel que $\sigma(a) = b$ (voir le lemme 10.10). On dira qu'un polynôme f est séparable s'il a « autant de racines (dans $\overline{K}$) que possible » (c'est-à-dire $\deg(f)$). On dira qu'une extension L/K est séparable si elle admet « autant de K-homomorphismes $L \to \overline{K}$ que possible » (notion à préciser ci-dessous).

Exemple 11.1. *(a) Le polynôme $X^2 - 2 \in \mathbb{Q}[X]$ a deux racines dans $\mathbb{C}$ et son degré est également 2.*

(b) Le polynôme $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ a quatre racines dans $\mathbb{C}$ et son degré est également 4.

(c) Soit p un nombre premier. Le polynôme $X^p - T \in \mathbb{F}_p(T)[X]$ (où $\mathbb{F}_p(T) := \mathrm{Frac}(\mathbb{F}_p[T])$) est irréductible (comme nous l'avons vu par le critère d'Eisenstein), mais, avec $t \in \overline{\mathbb{F}_p(T)}$ tel que $t^p = T$ on a $X^p - T = (X - t)^p$, donc il n'y a qu'une seule racine bien que le degré soit p.

Définition 11.2. *Soit K un corps et $\overline{K}$ une clôture algébrique de K. Soit $f \in K[X]$.*

(a) Une racine $a \in \overline{K}$ de f est dite de multiplicité *r si $(X - a)^r \mid f$ et $(X - a)^{r+1} \nmid f$.*

(b) Le polynôme f est dit séparable *si toutes ses racines (dans $\overline{K}$) sont de multiplicité 1. Il est clair que f est séparable si et seulement si le nombre de racines distinctes (dans $\overline{K}$) est égale au degré de f.*

(c) Si f n'est pas séparable, on l'appelle inséparable.

Lemme 11.3. *Soient K un corps et $f, g \in K[X]$.*

(a) Soit L/K une extension de corps. Soient $\mathrm{pgcd}_{K[X]}(f, g)$ le plus grand commun diviseur unitaire de f et g dans l'anneau principal $K[X]$, et $\mathrm{pgcd}_{L[X]}(f, g)$ l'analogue dans $L[X]$. Alors, $\mathrm{pgcd}_{K[X]}(f, g) = \mathrm{pgcd}_{L[X]}(f, g)$.

(b) Pour $f = \sum_{i=0}^{d} a_i X^i$ nous définissons la dérivée formelle $f'(X) := \sum_{i=1}^{d} i a_i X^{i-1}$. *Alors, on a*

$$(f+g)' = f' + g' \quad \text{et} \quad (fg)' = f'g + fg'.$$

Démonstration. (a) Par l'identité de Bézout nous avons

$$d_1 := \operatorname{pgcd}_{K[X]}(f,g) = f(X)a_1(X) + g(X)b_1(X)$$
$$d_2 := \operatorname{pgcd}_{L[X]}(f,g) = f(X)a_2(X) + g(X)b_2(X)$$

avec $a_1, b_1 \in K[X]$ et $a_2, b_2 \in L[X]$. Nous avons les divisibilités suivantes dans $L[X]$: $d_1 | f$, $d_1 \mid g$, donc $d_1 \mid d_2$; et de la même façon $d_2 | f$, $d_2 \mid g$, donc $d_2 \mid d_1$. Comme d_1 et d_2 sont unitaires, on obtient $d_1 = d_2$.
Alternativement, il suffit de noter que l'algorithme d'Euclide appliqué à deux polynômes dans $K[X]$ produit toujours un polynôme dans $K[X]$.
(b) C'est un calcul simple. (Noter que vous ne pouvez pas utiliser la règle d'Analyse 1 sauf pour les corps $\mathbb{R}$ et $\mathbb{C}$.) □

Proposition 11.4. *Soient K un corps, $\overline{K}$ une clôture algébrique et $f \in K[X]$ de degré ≥ 1.*

(a) Soit $a \in \overline{K}$ une racine de f. Alors, les assertions suivantes sont équivalentes :

- *(i) La multiplicité de a est $r > 1$.*
- *(ii) $f'(a) = 0$.*
- *(iii) $\operatorname{pgcd}_{K[X]}(f, f')(a) = 0$.*

(b) Soit f irréductible. Alors, les assertions suivantes sont équivalentes :

- *(i) f est séparable.*
- *(ii) $f' \neq 0$ (polynôme constant 0).*

Démonstration. (a) Soit $f(X) = (X-a)^r \cdot g(X)$ pour un polynôme $g \in \overline{K}[X]$ tel que $g(a) \neq 0$. Donc

$$f'(X) = (X-a)^{r-1} \cdot \big(r \cdot g(X) + (X-a) \cdot g'(X)\big) = (X-a)^{r-1} \cdot h(X)$$

et $h(a) = r \cdot g(a) \neq 0$. Notez que par le lemme 11.3 le pgcd peut être calculé dans $\overline{K}[X]$, où il est évident. Les équivalences sont donc claires.
(b) On remarque que l'irréductibilité de f et l'inégalité stricte $\deg(f') < \deg(f)$ impliquent

$$\operatorname{pgcd}(f, f') \sim \begin{cases} 1 & \text{si } f' \neq 0, \\ f & \text{si } f' = 0 \end{cases}$$

où on utilise le pgcd unitaire. L'équivalence en suit directement en utilisant (a). □

Définition 11.5. *On appelle* parfait *tout corps K pour lequel tout polynôme irréductible $f \in K[X]$ est séparable.*

Exemple 11.6. *(a) Tout corps de caractéristique* 0 *est parfait.*

Raison : Pour $f \in K[X]$ *de degré* ≥ 1*, on a toujours* $f' \neq 0$ *(le degré diminue par* 1*).*

(b) Tout corps algébriquement clos est parfait.

Raison : Les seuls polynômes irréductibles sont linéaires et donc trivialement séparables.

(c) Le corps $\mathbb{F}_p(T) = \mathrm{Frac}(\mathbb{F}_p[T])$ *n'est pas parfait.*

Raison : Le polynôme $X^p - T \in \mathbb{F}_p(T)[X]$ *est irréductible et inséparable.*

Définition 11.7. *Soit* L/K *une extension algébrique de corps.*

(a) On appelle séparable sur K *tout* $a \in L$ *tel que son polynôme minimal* $\mathrm{mipo}_a(X) \in K[X]$ *sur* K *est séparable.*

(b) On appelle séparable *toute extension algébrique* L/K *telle que tout* $a \in L$ *est séparable sur* K*.*

(c) Soit $\overline{K}$ *une clôture algébrique de* K*. On pose*

$$[L : K]_s := \#\mathrm{Hom}_K(L, \overline{K})$$

et on l'appelle le degré de séparabilité de l'extension L/K*.*

Noter que $[L : K]_s$ *est indépendant du choix de* $\overline{K}$ *car toute autre clôture algébrique de* K *est* K*-isomorphe à la clôture* $\overline{K}$ *que nous avons choisie.*

Lemme 11.8. *Soit* K *un corps,* $\overline{K}$ *une clôture algébrique de* K*,* $a \in \overline{K}$ *et* $f := \mathrm{mipo}_a \in K[X]$ *son polynôme minimal sur* K*. Alors :*

(a) $[K(a) : K]_s$ *est égal au nombre de zéros de* f *dans* $\overline{K}$*, donc* $[K(a) : K]_s \leq [K(a) : K] = \deg(f)$*.*

(b) a *est séparable sur* $K \Leftrightarrow [K(a) : K] = [K(a) : K]_s$*.*

Démonstration. Immédiat à cause de la bijection

$$\{b \in \overline{K} \mid f(b) = 0\} \longrightarrow \mathrm{Hom}_K(K(a), \overline{K}),$$

l'égalité $[K(a) : K] = \deg(f)$ et le fait que le nombre de racines d'un polynômes est inférieur ou égal au degré. □

Proposition 11.9. *Soient* $M/L/K$ *des extensions algébriques de corps. Le degré de séparabilité est multiplicatif :*

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

Démonstration. Soient $\overline{K}$ une clôture algébrique de K et

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i \mid i \in I\} \quad \text{et} \quad \mathrm{Hom}_L(M, \overline{K}) = \{\tau_j \mid j \in J\}.$$

On suppose que le premier ensemble est en bijection avec I et le deuxième en bijection avec J. Pour tout $i \in I$ on choisit une prolongation $\overline{\sigma}_i : \overline{K} \to \overline{K}$ de σ_i (possible par la proposition 10.12). Ces prolongations sont des isomorphismes.
On montre d'abord que $(i,j) \mapsto \overline{\sigma}_i \circ \tau_j$ définit une bijection entre $I \times J$ et l'ensemble $\{\overline{\sigma}_i \circ \tau_j \mid i \in I, j \in J\}$. Comme la surjectivité est claire, il suffit de montrer l'injectivité. Pour cela, soient $i,k \in I$ et $j,\ell \in J$ tels que $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_k \circ \tau_\ell$. Comme $\tau_j|_L = \tau_\ell|_L = \mathrm{id}_L$ on obtient d'abord $\sigma_i = \overline{\sigma}_i|_L = \overline{\sigma}_k|_L = \sigma_k$, donc $i = k$. On multipliant l'égalité $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_i \circ \tau_\ell$ par $\overline{\sigma}_i^{-1}$ on voit $\tau_j = \tau_\ell$, donc $j = \ell$, achévant la prevue de l'injectivité.
Montrons maintenant :

$$\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j \mid i \in I, j \in J\}.$$

L'inclusion « $\supseteq$ » est évidente. Regardons l'autre « $\subseteq$ ». Soit $\tau \in \mathrm{Hom}_K(M, \overline{K})$. On considère $\tau|_L \in \mathrm{Hom}_K(L, \overline{K})$; donc il existe un $i \in I$ tel que $\tau|_L = \sigma_i$. Notons que $\overline{\sigma}_i^{-1} \circ \tau|_L = \mathrm{id}_L$. Donc $\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_L(M, \overline{K})$, donc il existe $j \in J$ tel que $\overline{\sigma}_i^{-1} \circ \tau = \tau_j$, alors $\tau = \overline{\sigma}_i \circ \tau_j$, ce qu'il fallait démontrer.
Nous avons établi une bijection entre $I \times J$ et $\mathrm{Hom}_K(M, \overline{K})$, donc l'assertion de la proposition. □

Lemme 11.10. *Soient $M/L/K$ des extensions de corps.*

(a) Soit $a \in M$. Si a est séparable sur K, alors a est séparable sur L.

(b) Si M/K est séparable, alors M/L et L/K sont séparables.

Démonstration. (a) Soient $f \in K[X]$ et $g \in L[X]$ les polynômes minimaux de a sur K et sur L respectivement. Par hypothèse f est séparable. Comme g est un diviseur de f, alors g est aussi séparable, donc a est séparable sur L.
(b) La séparabilité de L/K est triviale, et celle de M/L suit de (a). □

Lemme 11.11. *Soient $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = L$ des extensions finies de corps telles que $[K_{i+1} : K_i]_s \leq [K_{i+1} : K_i]$ pour tout $0 \leq i \leq n-1$. Les assertions suivantes sont équivalentes :*

(i) $[L : K] = [L : K]_s$

(ii) Pour tout $0 \leq i \leq n-1$, on a $[K_{i+1} : K_i] = [K_{i+1} : K_i]_s$.

Démonstration. Par la multiplicativité du degré et du degré de séparabilité nous avons les égalités

$$[L : K] = \prod_{i=0}^{n-1} [K_{i+1} : K_i] \text{ et } [L : K]_s = \prod_{i=0}^{n-1} [K_{i+1} : K_i]_s$$

qui impliquent l'équivalence en vue de $[K_{i+1} : K_i]_s \leq [K_{i+1} : K_i]$. □

Proposition 11.12. *Soit L/K une extension finie de corps. Les assertion suivantes sont équivalentes :*

(i) L/K est séparable.

(ii) Il existe des éléments $a_1, \ldots, a_n \in L$ séparables sur K tels que $L = K(a_1, \ldots, a_n)$.

(iii) $[L : K] = [L : K]_s$.

Démonstration. « (i) $\Rightarrow$ (ii) » : Clair : tout ensemble fini de générateurs est composé d'éléments séparables car tout élément dans l'extension est séparable.
« (ii) $\Rightarrow$ (iii) » : Soit $K_0 = K$ et pour $1 \leq i \leq n$ on pose $K_i = K(a_1, \ldots, a_i)$ et on remarque $K_i = K_{i-1}(a_i)$. Les lemmes 11.8, 11.10 et 11.11 impliquent le résultat.
« (iii) $\Rightarrow$ (i) » : Soit $a =: a_1 \in L$. On choisit des éléments $a_2, a_3, \ldots, a_n \in L$ tels que $L = K(a_1, a_2, \ldots, a_n)$. Comme ci-dessus, soit $K_0 = K$ et pour $1 \leq i \leq n$ on pose $K_i = K(a_1, \ldots, a_i)$, donc $K_i = K_{i-1}(a_i)$. Encore par le lemme 11.11 nous obtenons $[K(a) : K]_s = [K(a) : K]$, donc a est séparable sur K par le lemme 11.8. □

Corollaire 11.13 (Transitivité de la séparabilité)**.** *Soient $M/L/K$ des extensions algébriques. Alors M/K est séparable si et seulement si M/L et L/K sont séparables.*

Démonstration. Une direction a été démontrée dans le lemme 11.10. Si les extensions sont finies, l'autre est une conséquence des égalités

$$[M : K] = [M : L] \cdot [L : K] = [M : L]_s \cdot [L : K]_s = [M : K]_s$$

et de la proposition 11.12.
On peut ramener le cas des extensions infinies à celui des extensions finies ainsi. Soit $a \in M$. Comme a est séparable sur L, son polynôme minimal $f \in L[X]$ est séparable. Soit K' l'extension de K engendrée par les coefficients de f. Il suit que $K'(a)/K'$ est séparable car le polynôme minimal de a sur K' est toujours f. Comme K'/K est une extensions finie engendrée par des éléments séparables, K'/K est séparable. Par le cas des extensions finies, nous concluons que $K'(a)/K$ est séparable, donc a est séparable sur K. Cela montre que M/K est séparable. □

Ajoutons encore une version infinie de la proposition précédente.

Corollaire 11.14. *Soit L/K une extension algébrique de corps. Elle est séparable si et seulement si elle est engendrée par des éléments séparables sur K.*

Démonstration. Soit $\{a_i\}_{i \in I} \subseteq L$ un ensemble de générateurs séparables (pour un ensemble I). Tout $b \in L$ se trouve déjà dans $K(a_j \mid j \in J) \subseteq L$ pour un sous-ensemble fini $J \subseteq I$. Ce corps est séparable par la proposition 11.12. □

Exemple 11.15. *Un élément $a \in L$ qui engendre une extension L/K, c'est-à-dire $L = K(a)$, est dit* primitif pour L/K.
Par exemple, $\sqrt{5} + \sqrt{10}$ est un élément primitif de $\mathbb{Q}(\sqrt{5}, \sqrt{10})/\mathbb{Q}$ et que $\sqrt[3]{2}\sqrt[4]{5}$ est un élément primitif de $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/\mathbb{Q}$.

Proposition 11.16 (Existence d'élément primitif)**.** *Soit K un corps infini et L/K une extension finie et séparable. Alors, il existe $a \in L$ tel que $L = K(a)$, donc L est une extension simple de K.*

Noter que le résultat est aussi vrai pour les corps finis ; mais la preuve en est différente (exercice).

Démonstration. Soit $\overline{K}$ une clôture algébrique de K. Sans perte de généralité nous pouvons supposer $L = K(b, c)$. Soient $f = \mathrm{mipo}_b$ et $g = \mathrm{mipo}_c$ les polynômes minimaux de b et c sur K et $b = b_1, b_2, \ldots, b_n, c = c_1, c_2, \ldots, c_m \in \overline{K}$ leurs zéros. Nous choisissons $y \in K$ tel que pour tout $1 \leq i \leq$

n et $2 \leq j \leq m$ nous avons $y \neq \frac{b_i - b}{c - c_j}$ (ici on utilise que K contient assez d'éléments) et nous posons $a := b + yc$.
On montre $b, c \in K(a)$, donc $K(a) = K(b, c)$.
Posons $h(X) := f(a - yX) \in K(a)[X]$. On a $h(c) = f(a - yc) = f(b) = 0$. Mais, $h(c_j) \neq 0$ pour tout $2 \leq j \leq m$ pour la raison suivante : Par choix de y nous avons $b_i - b \neq y(c - c_j)$ donc $b_i \neq b + yc - yc_j = a - yc_j$ pour tout $1 \leq i \leq n$. Alors, $h(c_j) = f(a - yc_j) \neq 0$ car $a - yc_j$ est différent de toutes les racines de f. Donc, $\mathrm{pgcd}_{K(a)[X]}(h, g) = X - c$, donc $c \in K(a)$, donc $b \in K(a)$. □

Corps finis

Lemme 11.17. *Soit K un corps fini (c'est-à-dire : $\#K < \infty$). Alors :*

(a) $\mathrm{car}(K) = p > 0$*, un nombre premier et l'homomorphisme naturel $\mathbb{F}_p \to K$ est injectif; donc on considère K comme une extension de $\mathbb{F}_p$.*

(b) Il existe $n \in \mathbb{N}$ tel que $\#K = p^n$.

(c) $\mathrm{Frob}_p : K \to K, \quad x \mapsto x^p$ *est un homomorphisme de corps, « l'homomorphisme de Frobenius » (voir la définition-lemme 7.7).*

Démonstration. Cela a déjà été démontré. Rappelons quand-même (b). Comme K est une extension de $\mathbb{F}_p$, c'est un $\mathbb{F}_p$-espace vectoriel de dimension $n = [K : \mathbb{F}_p]$ (forcement finie, car K est finie). Donc $K \cong (\mathbb{F}_p)^n$ en tant que $\mathbb{F}_p$-espace vectoriel. Donc $\#K = p^n$. □

Théorème 11.18. *Soit p un nombre premier et n un nombre naturel. Soit $f(X) := X^{p^n} - X \in \mathbb{F}_p[X]$.*

(a) Si K est un corps de cardinal p^n, alors K est un corps de décomposition de f sur $\mathbb{F}_p$.

(b) Tout corps de décomposition N de f sur $\mathbb{F}_p$ est un corps de cardinal p^n.

(c) Si K_1 et K_2 sont deux corps de cardinal p^n, alors ils sont isomorphes. On note $\mathbb{F}_{p^n}$ tout corps de cardinal p^n. (C'est justifié car il est unique à isomorphisme près.)

(d) $\mathbb{F}_{p^n}/\mathbb{F}_p$ est une extension de corps séparable et normale de degré n.

Attention ! Ne pas confondre $\mathbb{F}_{p^n}$ avec $\mathbb{Z}/p^n\mathbb{Z}$. Les deux sont différents dès que $n > 1$.

Démonstration. On fait la preuve en plusieurs étapes.

- La dérivée formelle de f est $f'(X) = -1$, donc $\mathrm{pgcd}(f, f') = 1$. Par la proposition 11.4 (a) tout zéro de f dans N est de multiplicité 1. Donc, f est séparable. En conséquence, $N/\mathbb{F}_p$ est séparable et le nombre de racines distinctes de f dans N est égal au degré du polynôme, donc égal à p^n.
- Soit K est un corps de cardinal p^n. Alors, $K^\times = K \setminus \{0\}$ est un groupe d'ordre $p^n - 1$. Alors pour tout $a \in K^\times$ on a : $a^{p^n - 1} = 1$, donc $a^{p^n} - a = 0$, donc, $f(a) = 0$. Evidemment, $f(0) = 0$. On conclut : $f(a) = 0$ pour tout $a \in K$. Donc, K est égal à l'ensemble des racines de f. On obtient que K est un corps de décomposition de f et donc (a).

- On veut montrer (b) maintenant. Soit N un corps de décomposition de f sur $\mathbb{F}_p$. On pose $R := \{a \in N \mid f(a) = 0\} \subseteq N$. Noter que $\#R = p^n$ à cause de la séparabilité de f.

- On montre que R est un sous-corps de N : Soient $a, b \in R$, donc $a^{p^n} = a$ et $b^{p^n} = b$. Cela implique :

  - $0^{p^n} = 0$ et $1^{p^n} = 1$, donc $0, 1 \in R$;
  - $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a+b$, donc $a+b \in R$ (on utilise l'additivité de l'homomorphisme de Frobenius) ;
  - $(-a)^{p^n} = (-1)^{p^n} a^{p^n} = -a$, donc, $-a \in R$ (noter que pour $p = 2$ il n'y a rien à démontrer et pour $p > 2$ on a $(-1)^{p^n} = -1$) ;
  - $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n} = a \cdot b$, donc $a \cdot b \in R$;
  - si $a \neq 0$, alors $\left(\frac{1}{a}\right)^{p^n} = \frac{1}{a^{p^n}} = \frac{1}{a}$, donc $\frac{1}{a} \in R$.

- Donc R est un sous-corps du corps de décomposition de f qui contient toutes les racines de f. Par la définition du corps de décomposition, on conclut $R = N$. Donc, $\#N = p^n$. Cela montre (b).

- (c) L'unicité provient du fait que les corps de décomposition sont uniques à isomorphisme près.

- (d) $\mathbb{F}_{p^n}/\mathbb{F}_p$ est normal, car c'est un corps de décomposition, et elle est séparable, car f l'est. Le cardinal implique l'assertion concernant le degré.

□

12 Extensions galoisiennes

Objectifs :

- Maîtriser la définition d'extension galoisienne et de son groupe de Galois,

- savoir décider si une extension donnée est galoisienne,

- savoir calculer le groupe de Galois d'extensions galoisiennes dans de petits cas,

- connaître le groupe de Galois d'une extension de corps finis,

- connaître la définition du sous-corps fixé par un sous-groupe du groupe de Galois et savoir le calculer dans des exemples simples,

- connaître et savoir appliquer le théorème principal de la théorie de Galois ainsi que ces corollaires,

- connaître des exemples et savoir démontrer des propriétés simples.

Soit L/K une extension normale. On se rappelle que par la proposition 10.20 tout élément σ de $\mathrm{Hom}_K(L, \overline{L})$ satisfait $\sigma(L) = L$ et donne donc lieu à un K-isomorphisme $L \to L$. On note l'ensemble des K-isomorphismes $L \to L$ par $\mathrm{Aut}_K(L)$. C'est clairement un groupe pour la composition d'applications avec élément neutre l'identité id_L.
Nous avons donc pour L/K une extension finie et normale

$$\#\,\mathrm{Aut}_K(L) = \#\mathrm{Hom}_K(L, \overline{L}) = [L : K]_s \leq [L : K] \tag{12.1}$$

avec égalité si et seuelement si L/K est aussi séparable.

Définition 12.1. *Soit L/K une extension algébrique. On appelle* galoisienne *toute extension algébrique L/K qui est normale et séparable. On pose*

$$\mathrm{Gal}(L/K) := G(L/K) := \mathrm{Aut}_K(L)$$

(l'ensemble des K-homomorphisme $L \to L$) et on l'appelle groupe de Galois de L/K.

Lemme 12.2. *Soit L/K une extension galoisienne finie. Alors $\#\,\mathrm{Gal}(L/K) = [L : K]$.*

Démonstration. Conséquence de l'équation (12.1) et de la séparabilité. □

Exemple 12.3. *(a) $\mathbb{C}/\mathbb{R}$ est une extension galoisienne : elle est normale (par exemple, car le degré est 2) et séparable (par exemple, car la caractéristique est 0).*

$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) = \{\mathrm{id}_{\mathbb{C}}, c\}$ *où c est la conjugaison complexe.*

(b) Soit $\mathbb{N} \ni d \neq 0, 1$ un nombre qui n'est pas un carré de façon que $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ est une extension de degré 2 qui est galoisienne. Nous avons :

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$$

où σ est déterminé uniquement par $\sigma(\sqrt{d}) = -\sqrt{d}$.

(c) Soient p un nombre premier et $\zeta_p := e^{2\pi i/p}$. On pose $K := \mathbb{Q}(\zeta_p)$ (le p-ième corps cyclotomique). Alors $K/\mathbb{Q}$ est une extension galoisienne. Son groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ est cyclique d'ordre $p - 1$.

En effet : Nous connaissons le polynôme minimal de ζ_p sur $\mathbb{Q}$. C'est le p-ième polynôme cyclotomique $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbb{Q}[X]$. Ses racines sont toutes les puissances ζ_p^j pour $j = 1, 2, \ldots, p - 1$. Donc il est clair que $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ est galoisienne.

Donc, nous pouvons directement écrire $p - 1$ homomorphismes $K \to K$:

$$\sigma_j : K \to K, \text{ déterminé uniquement par } \sigma_j(\zeta_p) = \zeta_p^j$$

pour $j \in \{1, 2, \ldots, p - 1\}$ et comme le cardinal de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ est $p - 1$, nous avons trouvé les éléments de ce groupe.

*Il faut encore voir que le groupe est cyclique. On rappelle que $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ est cyclique (par exemple, par un exercice). Nous définissons le p-*ième caractère cyclotomique *:*

$$\chi_p : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$$

comme suit : Soit $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. *Nous avons* $\tau(\zeta_p) = \zeta_p^{\chi(\tau)}$ *pour un* $\chi(\tau) \in (\mathbb{Z}/p\mathbb{Z})^\times$. *Cette application est clairement bijective. On calcule qu'il s'agit d'un homomorphisme (donc d'un isomorphisme) de groupes :*

$$\zeta_p^{\chi(\tau_1\tau_2)} = \tau_1(\tau_2(\zeta_p)) = \tau_1(\zeta_p^{\chi(\tau_2)}) = \big(\tau_1(\zeta_p)\big)^{\chi(\tau_2)} = \big(\zeta_p^{\chi(\tau_1)}\big)^{\chi(\tau_2)} = \zeta_p^{\chi(\tau_1)\chi(\tau_2)}.$$

Ce même résultat est valable pour tout entier positif n *et ne pas seulement pour les nombres premiers* p *(exercice).*

(d) Soit $\zeta_3 = e^{2\pi i/3}$. *On considère l'extension* $K := \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ *qui est galoisienne (la séparabilité est claire car nous sommes en caractéristique* 0*, et la normalité a été montrée dans un exemple précédent). Son degré est* 6. *On va maintenant calculer les éléments de son groupe de Galois* $\mathrm{Gal}(K/\mathbb{Q})$.

On va d'abord prolonger l'identité $\mathbb{Q} \hookrightarrow \mathbb{C}$ *à* $K' := \mathbb{Q}(\zeta_3)$*; c'est un cas spécial de l'exemple précédent : le polynôme minimal de* ζ_3 *est* $X^2 + X + 1 \in \mathbb{Q}[X]$ *et ses deux racines sont* ζ_3 *et* ζ_3^2. *Donc nous avons deux prolongations*

$$\sigma_i : \mathbb{Q}(\zeta_3) \to \mathbb{C}$$

données par $\sigma_1(\zeta_3) = \zeta_3$ *et* $\sigma_2(\zeta_3) = \zeta_3^2$. *(On sait que* $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ *est galoisien, mais on ne va pas utiliser ce fait.)*

Le polynôme $X^3 - 2$ *reste irréductible sur* $\mathbb{Q}(\zeta_3)[X]$ *(par exemple, par la multiplicativité des degrés et le fait que* 2 *et* 3 *sont premiers entre eux). Donc pour tout* $i \in \{1, 2\}$ *nous pouvons prolonger* σ_i *à* $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ *de trois manières qui sont déterminées par :*

$$\sigma_{i,1}(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \sigma_{i,2}(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}, \quad \sigma_{i,3}(\sqrt[3]{2}) = \zeta_3^2\sqrt[3]{2}.$$

Par la normalité de $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ *ces* $\mathbb{Q}$*-homomorphismes donnent des éléments dans le groupe de Galois* $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$. *Nous avons donc calculé les éléments du groupe de Galois. Notons encore que* $\sigma_{1,1}$ *est l'identité.*

(e) Soit K *un corps fini de caractéristique* p *et de cardinal* p^n. *Nous avons vu dans la section précédente que* $K/\mathbb{F}_p$ *est séparable et normal, donc, galoisien. Son degré est* n.

Nous calculons le groupe de Galois $\mathrm{Gal}(K/\mathbb{F}_p)$. *Pour cela on se rappelle du Frobenius* $\mathrm{Frob}_p : K \to K$ *donné par* $x \mapsto x^p$*; c'est un automorphisme de corps.*

Nous savons que $\mathrm{Frob}_p^n = \mathrm{id}_K$. *On veut montrer que* n *est l'ordre de* Frob_p. *Soit* $1 \leq i < n$*; supposons que* $\mathrm{Frob}_p^i = \mathrm{id}$. *Alors, tout élément de* K *satisfait* $x^{p^i} = x$, *donc* $K \subseteq \mathbb{F}_{p^i}$, *ce qui est une contradiction. Donc, l'ordre de* Frob_p *est bien* n.

Nous pouvons conclure que $\mathrm{Gal}(K/\mathbb{F}_p)$ *est un groupe cyclique d'ordre* p *engendré par* Frob_p.

(f) Soit K *un corps et* $f \in K[X]$ *un polynôme irréductible et séparable. Alors le corps de décomposition* L *de* f *sur* K *est une extension galoisienne de* K.

Raison : Elle est normale, et elle est engendrée par les racines de f*, donc par des éléments séparables. Nous nous rappelons que nous avons vu que les extensions engendrées par des éléments séparables sont séparables.*

Lemme 12.4. *Soient $L/E/K$ des extensions de corps telles que L/K est galoisienne. Alors :*

(a) L/E est galoisien et $\mathrm{Gal}(L/E)$ est le sous-groupe de $\mathrm{Gal}(L/K)$ composé des ces éléments de $\mathrm{Gal}(L/K)$ qui sont des E-homomorphismes (c'est-à-dire, $\sigma(e) = e$ pour tout $e \in E$).

(b) Si E/K est aussi galoisien (ce qui n'est pas automatique !), alors l'application

$$\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K), \quad \sigma \mapsto \sigma|_E$$

est un homomorphisme de groupes surjectif. Son noyau est égal à $\mathrm{Gal}(L/E)$.

Démonstration. (a) Nous avons vu les deux propriétés : normal (proposition 10.22) et séparable (lemme 11.10). Nous avons

$$\mathrm{Gal}(L/E) = \mathrm{Aut}_E(L) \subseteq \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K).$$

(b) Comme E/K est supposé normal, pour tout K-homomorphisme $\sigma : L \to L$ on a toujours $\sigma(E) = E$. Donc $\sigma|_E \in \mathrm{Gal}(E/K)$, et l'application π est bien définié. Il est clair que π est un homomorphisme.
On montre la surjectivité : Soit $\tau \in \mathrm{Gal}(E/K)$. En utilisant la proposition 10.12 on prolonge l'application

$$E \xrightarrow{\tau} E \hookrightarrow L \hookrightarrow \overline{L}$$

en un K-homomorphisme $\tilde{\tau} : L \to \overline{L}$. La normalité de L/K implique que $\tilde{\tau}(L) = L$, donc $\tilde{\tau}|_L \in \mathrm{Gal}(L/K)$ et satisfait $\pi(\tilde{\tau}) = \tau$.
Pour calculer le noyau de π, soit $\sigma \in \mathrm{Gal}(L/K)$. Par définition $\pi(\sigma) = \sigma|_E = \mathrm{id}_E$ si et seulement si $\sigma \in \mathrm{Gal}(L/E)$. □

Définition-Lemme 12.5. *Soit L un corps et $G \subseteq \mathrm{Aut}(L)$. On pose*

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

C'est un corps, appelé le sous-corps de L fixé par G *ou* le sous-corps des G-invariants de L.

Démonstration. Facile à vérifier. □

Par exemple, $\mathbb{R}$ est le sous-corps de $\mathbb{C}$ fixé par la conjugaison complexe.

Lemme 12.6. *Soient L un corps, $G \subseteq \mathrm{Aut}(L)$ un sous-groupe fini du groupe des automorphismes de L et $K := L^G$. Pour $a \in L$, on considère l'ensemble fini $S = \{\sigma(a) \mid \sigma \in G\}$. Alors, le polynôme minimal de a sur K est égal à $f = \prod_{s \in S}(X - s)$. Il est séparable de degré inférieur ou égal au cardinal de G.*

Démonstration. Puisque $\#S \leq \#G$ et les éléments d'un ensemble sont deux-à-deux distincts, la dernière assertion est claire. Comme $a = \mathrm{id}(a) \in S$, on a aussi $f(a) = 0$. Tout $\tau \in G$ se restreint en une bijection $S \to S$ car $\tau(\sigma(a)) = \tau \circ \sigma(a) \in S$ (l'inverse est donné par τ^{-1}). Cela veut dire que τ permute les facteurs du produit dans la définition de f, mais ne change pas f. En conséquence, $f^\tau = f$ pour tout $\tau \in G$, et donc $f \in K[X]$. Pour voir que f est irréductible, soit g l'unique diviseur irréductible et unitaire de f tel que $g(a) = 0$. Puisque G permute les racines de g, on a que $\sigma(a)$ est également une racine de g pour tout $\sigma \in G$. Cela implique $f = g$ et donc l'irréductibilité de f. □

Proposition 12.7. *Soient L un corps, $G \subseteq \mathrm{Aut}(L)$ un groupe fini et $K := L^G$. Alors L/K est une extension galoisienne avec $\mathrm{Gal}(L/K) = G$.*

Démonstration. Cette preuve se fait en plusieurs étapes :

- Notons que $G \leq \mathrm{Aut}_K(L)$. Nous avons par (12.1) :
$$n := \#G \leq \#\,\mathrm{Aut}_K(L) \leq [L : K].$$
- Soit $a \in L$. Par le lemme 12.6, le polynôme minimal f_a de a sur K est séparable et $\deg(f_a) \leq n$. Nous trouvons donc que tout élément $a \in L$ est séparable. Donc l'extension L/K est séparable. En plus, elle est normale parce que L est un corps de décomposition de la famille $\{f_a\}_{a\in L}$. Donc L/K est une extension galoisienne.
- Soit E un sous-corps de L qui contient K tel que E/K est une extension finie. Cette extension est séparable en tant que sous-extension d'une extension séparable. Soit $a \in E$ un élément primitif sur K, qui existe à cause de la proposition 11.16. Donc $E = K(a)$ et $[E : K] = \deg(f_a) \leq n$.

  Cela montre que toute extension finie E/K contenue dans L est de degré inférieur ou égal à n. Il en suit que $[L : K] \leq n$, en particulier, L/K est une extension finie.
- En comparant avec la prémière inégalité en haut, nous trouvons
$$G = \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K).$$

□

En fait, la preuve donne une manière d'écrire le polynôme minimal (voir exercices).

Corollaire 12.8. *Soit L/K une extension normale. On suppose que $G := \mathrm{Aut}_K(L)$ est fini. Alors :*

(a) L/L^G est une extension galoisienne avec $\mathrm{Gal}(L/L^G) = G$.

(b) $[L^G : K]_s = 1$.

(c) Si L/K est séparable (donc galoisien), alors $K = L^G$.

Démonstration. (a) C'est encore une fois l'assertion de la proposition 12.7.
(b) Il est clair que $K \leq L^G$. Nous avons la chaine d'inclusions
$$G = \mathrm{Gal}(L/L^G) = \mathrm{Aut}_{L^G}(L) \subseteq \mathrm{Aut}_K(L) = G,$$
donc nous avons l'égalité partout.
Soit $\overline{L}$ une clôture algébrique de L (qui est automatiquement aussi une clôture algébrique de K). Soit $\sigma : L^G \to \overline{L}$ un K-homomorphisme. On peut le prolonger à un K-homomorphisme $\tilde{\sigma} : L \to \overline{L}$ à cause de la proposition 10.12. La normalité de L/K implique $\tilde{\sigma}(L) = L$, donc $\tilde{\sigma} \in \mathrm{Aut}_K(L)$. On conclut $\tilde{\sigma} \in \mathrm{Aut}_{L^G}(L)$. Alors, $\tilde{\sigma}|_{L^G} = \sigma = \mathrm{id}_{L^G}$. Donc, $\mathrm{Hom}_K(L^G, \overline{L}) = \{\mathrm{id}_{L^G}\}$ et alors $[L^G : K]_s = 1$.
(c) Comme L/K est séparable, alors L^G/K l'est aussi. Donc $[L^G : K]_s = [L^G : K] = 1$ et $L^G = K$. □

Théorème 12.9 (Théorème principal de la théorie de Galois)**.** *Soient L/K une extension galoisienne finie et $G := \mathrm{Gal}(L/K)$. Alors :*

(a) Les applications

$$\begin{array}{ccc} \{H \mid H \leq G \text{ sous-groupe }\} & \overset{\Phi}{\underset{\Psi}{\rightleftarrows}} & \{E \mid E \text{ corps tel que } L/E/K\}, \\ H & \overset{\Phi}{\longmapsto} & L^H \\ \mathrm{Gal}(L/E) & \overset{\Psi}{\longmapsto} & E \end{array}$$

sont des bijections.

(b) Soit $H \subseteq G$ un sous-groupe. Alors

$$[L : L^H] = \#H \quad \text{et} \quad [L^H : K] = (G : H) = \frac{\#G}{\#H}.$$

(c) Soit E un corps tel que $L/E/K$. Alors

$$[L : E] = \#\,\mathrm{Gal}(L/E) \quad \text{et} \quad [E : K] = (\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)) = \frac{\#\,\mathrm{Gal}(L/K)}{\#\,\mathrm{Gal}(L/E)}.$$

(d) Soit $H \leq G$ un sous-groupe. Les assertions suivantes sont équivalentes :

(i) $H \lhd G$ est un sous-groupe normal.

(ii) L^H/K est une extension normale (donc galoisienne).

(e) Si L^H/K est normal, alors l'application

$$\pi : G \to \mathrm{Gal}(L^H/K), \quad \sigma \mapsto \sigma|_{L^H}$$

induit un isomorphisme de groupes $G/H \cong \mathrm{Gal}(L^H/K)$.

Démonstration. (a) On vérifie $\Phi \circ \Psi = \mathrm{id}$ et $\Psi \circ \Phi = \mathrm{id}$.
Soit E un corps tel que $L/E/K$. Alors :

$$\Phi(\Psi(E)) = \Phi(\mathrm{Gal}(L/E)) = L^{\mathrm{Gal}(L/E)} = E,$$

où la dernière égalité est due au corollaire 12.8 (c).
Soit $H \leq G$ un sous-groupe. Alors :

$$\Psi(\Phi(H)) = \Psi(L^H) = \mathrm{Gal}(L/L^H) = H,$$

où la dernière égalité a été démontrée dans le corollaire 12.8 (a).
(b) L'égalité $[L : L^H] = \#H$ provient directement du corollaire 12.8. L'autre égalité est une conséquence de la multiplicativité du degré : $[L^H : K] = \frac{[L:K]}{[L:L^H]} = \frac{\#G}{\#H} = (G : H)$.
(c) L'égalité $[L : E] = \#\,\mathrm{Gal}(L/E)$ exprime que L/E est normal et séparable. La deuxième suit par la multiplicativité du degré : $[E : K] = \frac{[L:K]}{[L:E]} = \frac{\#G}{\#Gal(L/E)}$.

(d) On fait d'abord un petit calcul : Soit $\sigma \in G$ et $H \leq G$ un sous-groupe. Alors

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

En effet : $a \in \sigma(L^H) \Leftrightarrow \sigma^{-1}(a) \in L^H \Leftrightarrow h \circ \sigma^{-1}(a) = \sigma^{-1}(a)$ pour tout $h \in H \Leftrightarrow \sigma \circ h \circ \sigma^{-1}(a) = a$ pour tout $h \in H \Leftrightarrow a \in L^{\sigma H \sigma^{-1}}$.
Nous pouvons maintenant démontrer l'assertion ainsi :

$$\begin{aligned} L^H/K \text{ est normal} &\overset{\text{prop. 10.20}}{\Leftrightarrow} && \sigma(L^H) = L^H \quad \forall\, \sigma \in G \\ &\Leftrightarrow && L^{\sigma H \sigma^{-1}} = L^H \quad \forall\, \sigma \in G \\ &\overset{\text{(a)}}{\Leftrightarrow} && H = \sigma H \sigma^{-1} \quad \forall\, \sigma \in G \\ &\overset{\text{déf.}}{\Leftrightarrow} && H \lhd G \text{ est un sous-groupe normal.} \end{aligned}$$

(e) Par le théorème d'isomorphisme, le lemme 12.4 nous donne pour le corps L^H :

$$G/H \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L^H) \xrightarrow{\pi\ \sim} \mathrm{Gal}(L^H/K).$$

□

Exemple 12.10. *(a) Soit L/K une extension galoisienne dont le groupe de Galois $G = \mathrm{Gal}(L/K)$ est cyclique de cardinal 6, donc isomorphe à $\mathbb{Z}/6\mathbb{Z}$. La liste complète des sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ est la suivante : $\{0\}, 3\mathbb{Z}/6\mathbb{Z}, 2\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$. Donc il y a 4 sous-corps de L/K dont les degrés sur K sont 6, 3, 2, 1.*

(b) Nous avons déjà calculé le groupe de Galois de $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$.

On calcule maintenant tous les sous-corps de $K := \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Par un exercice, le groupe de Galois $G := \mathrm{Gal}(K/\mathbb{Q})$ est isomorphe au groupe symétrique S_3.

Plus précisement : Nous prenons les deux homomorphismes $\sigma, \tau : K \to K$ déterminés uniquement par :

$$\sigma(\zeta_3) = \zeta_3^2, \quad \sigma(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\zeta_3) = \zeta_3, \quad \tau(\sqrt[3]{2}) = \zeta_3 \sqrt[3]{2}.$$

L'ordre de σ est 2 et l'ordre de τ est 3. Ces deux éléments engendrent G. Voici la liste des sous-groupes de G et des corps fixés par ces groupes.

- $H := \{\mathrm{id}\}$, $K^H = K$.
- $H := G$, $K^H = \mathbb{Q}$.
- $H := \langle\tau\rangle \lhd G$ *est un sous-groupe normal (car l'indice est 2 ; c'est le groupe alterné $A_3 \lhd S_3$),* $K^H = \mathbb{Q}(\zeta_3)$.
- $H := \langle\sigma\rangle \leq G$, $K^H = \mathbb{Q}(\sqrt[3]{2})$.
- $H := \langle\tau\sigma\tau^{-1}\rangle \leq G$, $K^H = \tau(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\tau(\sqrt[3]{2})) = \mathbb{Q}(\zeta_3\sqrt[3]{2})$.
- $H := \langle\tau^2\sigma\tau^{-2}\rangle \leq G$, $K^H = \tau^2(\mathbb{Q}(\sqrt[3]{2})) = \mathbb{Q}(\tau^2(\sqrt[3]{2})) = \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$.

(c) Soit K un corps fini de caractéristique p et de cardinal p^n. Nous avons vu que $\mathrm{Gal}(K/\mathbb{F}_p)$ est cyclique d'ordre n engendré par le Frobenius Frob_p.

Donc $\mathrm{Gal}(K/\mathbb{F}_p)$ est isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$. Les sous-groupes sont précisement donnés par $a\mathbb{Z}/n\mathbb{Z}$ pour $a \mid n$. La théorie de Galois nous redonne donc le résultat que les sous-corps de $\mathbb{F}_{p^n}$ sont précisement $\mathbb{F}_{p^n}^{\langle \mathrm{Frob}_p^a \rangle} = \mathbb{F}_{p^a}$ pour les diviseurs a de n.

(d) Soit L/K une extension (finie) de corps finis. Soit p^n le cardinal de L. Donc L/K est une extension galoisienne de groupe de Galois cyclique $\langle \mathrm{Frob}_p^a \rangle$ où p^a est le cardinal de K.

Voici un corollaire simple mais pas évident !

Corollaire 12.11. *Soit L/K une extension séparable et finie. Alors, l'ensemble*

$$\{E \text{ corps} \mid L/E/K \text{ extensions de corps}\}$$

est fini.

Démonstration. Sans perte de généralité nous pouvons remplacer L par une clôture normale. Donc, on peut supposer que L/K est une extension galoisienne. Il est clair que son groupe de Galois $\mathrm{Gal}(L/K)$ qui est un groupe fini ne possède qu'un nombre fini de sous-groupes (déjà l'ensemble des sous-ensembles de G est fini). Donc par le théorème 12.9 il n'existe qu'un nombre fini de corps E tels que $L/E/K$. □

Proposition 12.12. *Soit L/K une extension de corps. Soient $L/L_1/K$ et $L/L_2/K$ des extensions telles que L_1/K et L_2/K sont galoisiennes et finies.*

(a) Le corps $L_1L_2 := K(L_1, L_2)$ (extension de K dans L engendrée par les éléments de L_1 et L_2) est une extension galoisienne et finie de K.

(b) La restriction

$$\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/(L_1 \cap L_2)), \quad \sigma \mapsto \sigma|_{L_1}$$

est un isomorphisme de groupes.

(c) L'application

$$\varphi : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \quad \sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$$

est un homomorphisme de groupes injectif d'image

$$\mathrm{im}(\varphi) = \{(\sigma, \tau) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \mid \sigma|_{L_1 \cap L_2} = \tau|_{L_1 \cap L_2}\}.$$

Démonstration. Exercice. □

Définition 12.13. *On appelle* abélienne (cyclique) *toute extension galoisienne L/K telle que son groupe de Galois $\mathrm{Gal}(L/K)$ est abélien (cyclique).*

Corollaire 12.14. *Soient L_i/K pour $1 \leq i \leq n$ des extensions abéliennes contenu dans un corps L. Alors, l'extension $L_1 \cdots L_n/K$ est aussi une extension abélienne.*

Démonstration. Par la proposition 12.12 et récurrence, $\mathrm{Gal}(L_1 \cdots L_n/K)$ est un sous-groupe de $\prod_{i=1}^n \mathrm{Gal}(L_i/K)$ qui est abélien. Donc $\mathrm{Gal}(L_1 \cdots L_n/K)$ est abélien. □

13 Résolubilité par radicaux

Objectifs :

- Connaître la définition de la résolubilité d'une équation polynomielle par radicaux,
- maîtriser sa formulation en termes d'extensions de corps,
- connaître et maîtriser la définition de groupe résoluble, en connaître des exemples et des contre-exemples,
- connaître la définition de sous-groupe des commutateurs et de l'abélienisation d'un groupe,
- connaître le groupe de Galois des extensions cyclotomiques,
- connaître le groupe de Galois de l'équation générale de degré n,
- connaître la caractérisation de la résolubilité par radicaux de l'équation générale de degré n,
- connaître des exemples et savoir démontrer des propriétés simples.

Dans cette section nous regardons la motiviation de Galois pour sa théorie, la résolubilité des équations polynômiaux par radicaux.

- $f(X) := X^2 + aX + b \in \mathbb{Q}[X]$. Nous avons

  $$f(x) = 0 \Leftrightarrow x = \frac{1}{2}(-a \pm \sqrt{a^2 - 4b}),$$

  donc les racines de f peuvent être exprimées par des expressions « radicales », autrement dit, les racines de f appartiennent à une extension de $\mathbb{Q}$ qui peut être engendrée par des radicaux.

- $f(X) := X^3 + 3aX + 2b \in \mathbb{Q}[X]$. Soit $\zeta := \zeta_3 := e^{2\pi i/3}$. Nous avons

  $$f(x) = 0 \Leftrightarrow x = u + v \text{ ou } x = \zeta^2 u + \zeta v \text{ ou } x = \zeta u + \zeta^2 v,$$

  où $u = \sqrt[3]{-b + \sqrt{b^2 + a^3}}$ et $v = \sqrt[3]{-b - \sqrt{b^2 + a^3}}$. Donc ici aussi les racines de f peuvent être exprimées par des expressions « radicales », autrement dit, les racines de f appartiennent à une extension de $\mathbb{Q}$ qui peut être engendrée par des radicaux.

- Il existe aussi une formule en termes de radicaux pour les polynômes de degré 4.

Définition 13.1. *Soient K un corps parfait et $\overline{K}$ une clôture algébrique de K.*

(a) Une extension finie L/K est dite résoluble par radicaux *s'il existe des corps*

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$$

tels que

- $L \subseteq E_n$ *et*

- *pour tout* $1 \leq i \leq n$ *il existe* $a_i \in E_{i-1}$ *et* $n_i \in \mathbb{N}$ *tels que* $E_i = E_{i-1}(\sqrt[n_i]{a_i})$ *ou* $E_i = E_{i-1}(\zeta_{n_i})$ *où* $\zeta_{n_i} \in \overline{K}$ *est tel que* $\zeta_{n_i}^{n_i} = 1$.

(b) Une équation polynômielle $f(x) = 0$ *avec* $f(X) \in K[X]$ *est dite* résoluble par radicaux sur K *si un corps de décomposition de* f *sur* K *est résoluble par radicaux sur* K.

Cela veut dire que les racines de f *(qui appartiennent, comme on le sait, au corps de décomposition) peuvent être exprimées par une formule qui n'utilise que les éléments de* K *et les opérations* $+, -, \cdot, /, \sqrt[m]{\ }$ *pour* $m \in \mathbb{N}$.

Définition-Lemme 13.2. *Soient* K *un corps parfait et* $n \in \mathbb{N}_{>0}$. *Soit* μ_n *l'ensemble des racines (dans une clôture algébrique* $\overline{K}$ *de* K*) du polynôme* $X^n - 1 \in K[X]$. *On appelle* μ_n le groupe des n-ièmes racines de l'unité. *C'est un groupe cyclique (pour la multiplication de* K*).*
Alors $K(\mu_n)$ *est galoisien sur* K *et le groupe de Galois* $\mathrm{Gal}(K(\mu_n)/K)$ *est un groupe abélien.*
On appelle $K(\mu_n)$ *la* n-ième extension cyclotomique de K.

Démonstration.

- μ_n est un groupe : Soient $a, b \in \mu_n$, donc $a^n = b^n = 1$. Alors, $\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n} = 1$, donc $\frac{a}{b} \in \mu_n$. On en conclut que μ_n est un groupe.

- Que μ_n est cyclique provient de l'exercice qui dit que tout sous-groupe fini de $K^\times$ est cyclique.

- L'extension $K(\mu_n)/K$ est galoisienne : séparable car K est parfait et normale car c'est le corps de décomposition du polynôme $X^n - 1 \in K[X]$.

- L'application
$$\phi : \mathrm{Gal}(K(\mu_n)/K) \to \mathrm{Aut}(\mu_n), \quad \sigma \mapsto (\zeta \mapsto \sigma(\zeta))$$
est un homomorphisme de groupes injectif. Ici, $\mathrm{Aut}(\mu_n)$ est l'ensemble des automorphismes du groupe μ_n, c'est-à-dire l'ensemble des isomorphismes de groupes $\mu_n \to \mu_n$.

  Cette assertion est claire.

- $\mathrm{Aut}(\mu_n)$ est un groupe abélien : Comme μ_n est cyclique, on peut choisir un générateur $\zeta \in \mu_n$ et tout automorphisme $\sigma \in \mathrm{Aut}(G)$ est uniquement déterminé par $\sigma(\zeta)$. On a $\sigma(\zeta) = \zeta^m$ pour un $m \in \mathbb{N}$. Le groupe est abélien car la composition de deux automorphismes multiplie les exposants, et la multiplication dans $\mathbb{Z}$ est commutative.

□

Nous exposons maintenant les débuts de la « théorie de Kummer ». Dans la suite, si K est un corps et $a \in K$, on comprend par $K(\sqrt[n]{a})$ un corps de rupture du polynôme $X^n - a \in K[X]$. En général, c'est un choix.

Lemme 13.3. *Soient* K *un corps parfait,* $a \in K$ *et* $n \in \mathbb{N}_{>0}$. *Soit* $L := K(\sqrt[n]{a})$. *On suppose que* K *contient* μ_n.
Alors l'extension L/K *est galoisienne et le groupe de Galois* $\mathrm{Gal}(L/K)$ *est un sous-groupe de* μ_n *et donc cyclique (et abélien).*

Démonstration. L'extension L/K est galoisienne, car elle est séparable (comme K est parfait) et normale (c'est un corps de décomposition de $X^n - a$; ici on utilise que μ_n appartient à K). On définit l'application de Kummer

$$\psi : \mathrm{Gal}(L/K) \to \mu_n, \quad \sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

Elle est clairement injective car les K-homomorphismes $L \to L$ sont déterminés par l'image de $\sqrt[n]{a}$. C'est un homomorphisme de groupes :

$$\psi(\sigma \circ \tau) = \frac{\sigma(\tau(\sqrt[n]{a}))}{\sqrt[n]{a}} = \frac{\sigma(\psi(\tau)\sqrt[n]{a})}{\sqrt[n]{a}} = \psi(\tau)\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \psi(\tau)\psi(\sigma) = \psi(\sigma)\psi(\tau)$$

où on a utilisé que τ agit trivialement sur μ_n, donc sur l'image de ψ. □

Lemme 13.4. *Soit K un corps parfait. Soit L/K une extension galoisienne finie de groupe de Galois $G := \mathrm{Gal}(L/K)$. Supposons $\mu_n \subseteq L$. Soit $a \in L$. Soit N/K la clôture normale sur K (donc N/K est galoisien) de $L(\sqrt[n]{a})$ (vu comme un sous-corps d'une clôture algébrique de L).*
Alors, N/L est une extension abélienne.

Démonstration. On définit le polynôme

$$f(X) := \prod_{\sigma \in G} (X^n - \sigma(a)) \in L[X].$$

Comme il est clairement invariant par tout $\tau \in G$, il en suit que $f \in K[X]$. Ses racines sont $\zeta_n^i \sqrt[n]{\sigma(a)}$ pour $0 \leq i \leq n-1$ et $\sigma \in G$ où ζ_n est un générateur (fixé) de μ_n et $\sqrt[n]{\sigma(a)}$ est un choix fixé de racine de $X^n - \sigma(a)$.
Pour tout $\sigma \in G$, soit $\tilde{\sigma} : N \to N$ une prolongation. Alors on a $\left(\tilde{\sigma}(\sqrt[n]{a})\right)^n = \tilde{\sigma}(a) = \sigma(a)$. Il en suit que N contient une n-ième racine de $\sigma(a)$ pour tout $\sigma \in G$ et donc toutes les n-ièmes racines car $\mu_n \subseteq L$.
Soit M le corps de décomposition de f sur K. L'extension M/K est galoisienne, engendrée par μ_n et $\sqrt[n]{\sigma(a)}$ pour $\sigma \in G$. Le compositum de M et L est aussi une extension galoisienne de K. Donc $M = N$ car N est une extension galoisienne de K minimal contenant L et $\sqrt[n]{\sigma(a)}$ pour $\sigma \in G$.
On peut donc voir N comme le compositum de tous les corps $L(\sqrt[n]{\sigma(a)})$ pour $\sigma \in G$, donc $N = L(\sqrt[n]{\sigma(a)} : \sigma \in G)$. Par le corollaire 12.14 et le lemme 13.3 on obtient qu'en effet N/L est abélien.
□

Définition 13.5. *Soit G un groupe fini. On dit qu'il est* résoluble *s'il existe une suite de sous-groupes*

$$G_n = \{1\} \leq G_{n-1} \leq G_{n-2} \leq \cdots \leq G_1 \leq G_0 = G$$

telle que

- *pour tout $1 \leq i \leq n$ on a $G_i \lhd G_{i-1}$ (sous-groupe normal) et*
- *G_{i-1}/G_i est un groupe abélien.*

Théorème 13.6. *Soient K un corps parfait et L/K une extension finie qui est résoluble par radicaux. Alors, il existe une extension finie et galoisienne N/K telle que*

- $L \subseteq N$ *et*
- *le groupe de Galois* $\mathrm{Gal}(N/K)$ *est résoluble.*

Démonstration. Par définition nous avons des corps

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n$$

tels que

- $L \subseteq E_n$ et
- pour tout $1 \leq i \leq n$ il existe $a_i \in E_{i-1}$ et $n_i \in \mathbb{N}$ tels que $E_i = E_{i-1}(\sqrt[n_i]{a_i})$ ou $E_i = E_{i-1}(\zeta_{n_i})$.

On pose $M := \mathrm{ppcm}(n_i \mid 0 \leq i \leq n)$ et on définit $L_0 := K(\mu_M)$ (et $L_{-1} := K$). Alors $\mu_{n_i} \subseteq L_0$ pour tout $0 \leq i \leq n$ et L_0/K est une extension abélienne par la définition-lemme 13.2. Pour tout $1 \leq i \leq n$ on définit récursivement L_i comme la clôture normale sur K de $L_{i-1}E_i$. Par le lemme 13.4 L_i/L_{i-1} est abélien, c'est-à-dire $\mathrm{Gal}(L_i/L_{i-1})$ est abélien.
Le corps recherché est $N := L_n$. Par construction nous avons

$$\mathrm{Gal}(L_n/L_n) \trianglelefteq \mathrm{Gal}(L_n/L_{n-1}) \trianglelefteq \mathrm{Gal}(L_n/L_{n-2}) \trianglelefteq \cdots \trianglelefteq \mathrm{Gal}(L_n/L_0) \trianglelefteq \mathrm{Gal}(L_n/L_{-1})$$

et tous les quotients $\mathrm{Gal}(L_n/L_{i-1})/\mathrm{Gal}(L_n/L_i) \cong \mathrm{Gal}(L_i/L_{i-1})$ pour $0 \leq i \leq n$ sont des groupes abéliens. Donc $\mathrm{Gal}(L_n/L_{-1}) = \mathrm{Gal}(N/K)$ est un groupe résoluble. □

Remarque 13.7. *Par la théorie de Kummer on peut montrer que l'assertion réciproque tu théorème est également vraie : Si K est un corps parfait et N/K est une extension finie et galoisienne de groupe de Galois résoluble, alors toute extension L/K avec $L \subseteq N$ est résoluble par radicaux.*

Définition 13.8. *Soit G un groupe.*

(a) Soient $a, b \in G$. On dit que l'élément $[a, b] := aba^{-1}b^{-1} \in G$ est le commutateur de a, b.

(b) Soient $H_1, H_2 \leq G$ des sous-groupes.

$$[H_1, H_2] := \langle [a, b] \mid a \in H_1, b \in H_2 \rangle.$$

(c) $DG := G' := [G, G]$ est appelé le sous-groupe des commutateurs de G.

(d) Pour $i \geq 0$ on définit $D^iG := \underbrace{DD \ldots D}_{i\text{-fois}} G$.

Proposition 13.9. *Soit G un groupe.*

(a) $[G, G] \trianglelefteq G$ est un sous-groupe normal.

(b) Pour tout $N \trianglelefteq G$ sous-groupe normal :

$$G/N \text{ est abélien } \Leftrightarrow [G, G] \subseteq N.$$

(c) Les assertions suivantes sont équivalentes :

(i) G *est résoluble.*

(ii) Il existe $i \in \mathbb{N}$ *tel que* $D^iG = \{1\}$.

(d) Soit $H \trianglelefteq G$ *un sous-groupe distingué. Si* G *est résoluble, alors* G/H *est résoluble.*

Démonstration. (a) D'abord on remarque que $[G, G]$ est l'ensemble de tous les produits finis de commutateurs car $[a, b][b, a] = aba^{-1}b^{-1}bab^{-1}a^{-1} = 1$. Pour voir que $[G, G]$ est un sous-groupe normal de G il suffit donc de faire le calcul suivant :

$$g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}] \in [G, G]$$

pour tout $g, a, b \in G$.
(b) « $\Rightarrow$ » : Supposons que G/N est abélien. Alors, $1 = [aN, bN] = [a, b]N$. Donc $[a, b] \in N$ pour tout $a, b \in G$.
« $\Leftarrow$ » : Supposons que $[G, G] \subseteq N$. Donc, $aba^{-1}b^{-1} \in N$, donc $abN = baN$ pour tout $a, b, \in G$, montrant que G/N est abélien.
(c) « (i) $\Rightarrow$ (ii) » : Supposons que G est résoluble. Alors, il existe des sous-groupes

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq G_{n-2} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

tels que G_i/G_{i+1} est abélien pour tout $0 \leq i \leq n - 1$.
On démontre par récurrence $D^iG \subseteq G_i$ (ce qui implique $D^nG = \{1\}$).
Pour $i = 0$, on a $D^iG = G \subseteq G_0 = G$. Supposons l'assertion vraie pour i. On la démontre pour $i + 1$. Comme G_i/G_{i+1} est abélien, on obtient de (b) que $DG_i \subseteq G_{i+1}$. Par hypothèse $D^iG \subseteq G_i$, donc $D^{i+1}G = D(D^iG) \subseteq DG_i \subseteq G_{i+1}$.
« (ii) $\Rightarrow$ (i) » : On pose $G_i = D^iG$. La suite des G_i pour $i = 0, \ldots, n$ satisfait aux conditions car $G_n = \{1\}$ par l'hypothèse (ii), $G_0 = G$ et $G_i/G_{i+1} = D^iG/D(D^iG) = G_i/[G_i, G_i]$ est abélien.
(d) Cela suit directement de $D(G/H) = (DG)H/H$. □

Proposition 13.10. *Soit* $n \in \mathbb{N}_{>0}$.

(a) Le groupe symétrique S_n *est engendré par les transpositions* $(i \quad j)$ *pour* $i, j \in \{1, 2, \ldots, n\}$ *distincts.*

(b) Le groupe alterné A_n *est engendré par les* 3*-cycles* $(i \;\; j \;\; k)$ *pour* $i, j, k \in \{1, 2, \ldots, n\}$ *distincts.*

(c) $[S_n, S_n] = A_n$.

(d)
$$[A_n, A_n] = \begin{cases} \{1\} & \text{si } n = 1, 2, 3, \\ \{(1), (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\} & \text{si } n = 4, \\ A_n & \text{si } n \geq 5. \end{cases}$$

(e) Les groupes S_n *et* A_n *sont résolubles si et seulement si* $n \leq 4$.

Démonstration. (a) C'est une conséquence directe du calcul

$$(a_1 \ a_2 \ \dots \ a_r) = (a_1 \ a_2) \circ (a_2 \ a_3) \circ \cdots \circ (a_{r-1} \ a_r).$$

(b) Par (a) tout $\sigma \in A_n$ est le produit d'un nombre pair de transpositions. Donc il faut considérer les produits de deux transpositions et les exprimer en 3-cycles. Ça marche ainsi :

- $(a_1 \ a_2) \circ (a_3 \ a_4) = (a_1 \ a_3 \ a_2) \circ (a_1 \ a_3 \ a_4)$ si a_1, a_2, a_3, a_4 sont distincts.
- $(a_1 \ a_2) \circ (a_2 \ a_3) = (a_1 \ a_2 \ a_3)$ si a_1, a_2, a_3 sont distincts.
- $(a_1 \ a_2) \circ (a_1 \ a_2) = (1)$ si a_1, a_2 sont distincts.

(c) Comme S_n/A_n est abélien (isomorphe à $\mathbb{Z}/2\mathbb{Z}$ si $n \geq 3$ par la signature), on a par la proposition 13.9 que $[S_n, S_n] \subseteq A_n$. Soit $(a_1 \ a_2 \ a_3)$ un 3-cycle. On a

$$(a_1 \ a_2 \ a_3) = (a_1 \ a_3)(a_2 \ a_3)(a_1 \ a_3)^{-1}(a_2 \ a_3)^{-1} = [(a_1 \ a_3), (a_2 \ a_3)] \in [S_n, S_n].$$

Comme tout élément de A_n est un produit de 3-cycles, on obtient $A_n \subseteq [S_n, S_n]$.
(d) $n = 1, 2, 3, 4$ sont vérifiés par des calculs directs. Pour $n \geq 5$ il suffit d'exprimer tout 3-cycle $(a_1 \ a_2 \ a_3)$ comme un commutateur. C'est facile car on peut choisir a_4, a_5 tels que a_1, a_2, a_3, a_4, a_5 sont distincts et l'on a

$$(a_1 \ a_2 \ a_3) = (a_1 \ a_2 \ a_4)(a_1 \ a_3 \ a_5)(a_1 \ a_2 \ a_4)^{-1}(a_1 \ a_3 \ a_5)^{-1} = [(a_1 \ a_2 \ a_4), (a_1 \ a_3 \ a_5)].$$

(e) Pour $n \geq 5$ la proposition 13.9 montre que S_n et A_n ne sont pas résolubles. Les cas $n = 1, 2, 3, 4$ sont vérifiés par des calculs directs et faciles. □

Corollaire 13.11. *Soient K un corps parfait, $f \in K[X]$ un polynôme et N un corps de décomposition de f sur K. Si $\mathrm{Gal}(N/K)$ est isomorphe à S_n ou A_n pour un $n \geq 5$, alors f n'est pas résoluble par radicaux.*

Démonstration. Supposons f résoluble par radicaux. Par le théorème 13.6, cela revient à dire qu'il existe une extension galoisienne M/K qui contient N et tel que $\mathrm{Gal}(M/K)$ est résoluble. Donc $\mathrm{Gal}(N/K) = \mathrm{Gal}(M/K)/\mathrm{Gal}(M/N)$ est résoluble par la proposition 13.9(d). Cela contredit la proposition 13.10. □

Définition 13.12. *Soient K un corps et $K[A_0, \dots, A_{n-1}]$ l'anneau des polynômes à coefficients dans K pour les variables $A_0, \dots, A_{n-1}$. Soit $L := K(A_0, \dots, A_{n-1}) := \mathrm{Frac}(K[A_0, \dots, A_{n-1}])$ son corps des fractions. Le* polynôme général de degré n sur K *est*

$$f(X) := \sum_{i=0}^{n-1} A_i X^i + X^n \in L[X].$$

C'est donc le polynôme unitaire de degré n dont les coefficients sont les variables $A_0, \dots, A_{n-1}$.

La raison pour regarder le polynôme général est que les formules connues pour exprimer les zéros des équations polynomielles par radicaux font intervenir les coefficients du polynôme de départ ; c'est donc naturel de considérer ces coefficients comme des variables : dans la formule $x = \frac{-a \pm \sqrt{a^2-4b}}{2}$ pour $x^2 + ax + b = 0$, on considère a, b comme des variables.
Calculons maintenant le groupe de Galois du polynôme général de degré $n \in \mathbb{Z}_{>0}$.

Proposition 13.13. *Soit K un corps et soit $K[t_1, \ldots, t_n]$ l'anneau des polynômes dans les variables $t_1, \ldots, t_n$. Soit $\sigma \in S_n$ une permutation de l'ensemble $\{1, \ldots, n\}$. On obtient l'isomorphisme d'anneaux*

$$\sigma : K[t_1, \ldots, t_n] \to K[t_1, \ldots, t_n], \quad f(t_1, \ldots, t_n) \mapsto f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}),$$

donné par la permutation des variables par σ. En plus, σ donne un isomorphisme de corps $\sigma : N \to N$ par passage au corps des fractions $N := K(t_1, \ldots, t_n) := \mathrm{Frac}(K[t_1, \ldots, t_n])$. Cette construction nous permet de voir S_n comme sous-groupe de $\mathrm{Aut}(N)$.
Soit $L = N^{S_n}$.
Nous avons donc l'extension galoisienne N/L de groupe de Galois $\mathrm{Gal}(N/L) \cong S_n$.
Soit

$$f(X) := \prod_{i=1}^{n}(X - t_i) = \sum_{i=0}^{n-1} A_i X^i + X^n \in N[X].$$

(a) Le polynôme f appartient à $L[X]$, en particulier $A_0, \ldots, A_{n-1} \in L$.

(b) Le sous-anneau $K[A_0, \ldots, A_{n-1}] \subseteq L$ est isomorphe à l'anneau des polynômes à n variables, c'est-à-dire que l'application $K[X_0, \ldots, X_{n-1}] \xrightarrow{X_i \mapsto A_i} K[A_0, \ldots, A_{n-1}]$ est un isomorphisme.

(c) $L = K(A_0, \ldots, A_{n-1}) = \mathrm{Frac}(K[A_0, \ldots, A_{n-1}])$.

(d) Le polynôme f est le polynôme général de degré n sur K et N est un corps de décomposition de f sur L.

Démonstration. (a) On vérifie comme plusieurs fois avant que le polynôme f est invariant par tout $\sigma \in S_n$ car σ permute les facteurs $\prod_{i=1}^{n}(X - t_i)$. En conséquence, les coefficients A_i de f appartiennent à $L = N^{S_n}$.
(b) Nous suivons de près la démonstration de la proposition 6.22 (sauf que la numérotation change). Pour montrer que $K[A_0, \ldots, A_{n-1}]$ est isomorphe à un anneau des polynômes à n variables, il suffit de démontrer que tout polynôme $g \in K[X_0, \ldots, X_{n-1}]$ tel que $g(A_0, \ldots, A_{n-1}) = 0$ est égal à 0. On utilise récurrence en n. Le cas $n = 0$ est trivial. Supposons le résultat vrai pour $n - 1$ variables et considérons g en tant que polynôme dans $(K[X_1, \ldots, X_{n-1}])[X_0]$:

$$0 \neq g(X_0, \ldots, X_{n-1}) = g_0(X_1, \ldots, X_{n-1}) + g_1(X_1, \ldots, X_{n-1})X_0 \\ + g_2(X_1, \ldots, X_{n-1})X_0^2 + \cdots + g_r(X_1, \ldots, X_{n-1})X_0^r.$$

Supposons $g(A_0, \ldots, A_{n-1}) = 0$ et que le degré r soit minimal parmi les polynômes tels que nous avons $g(A_0, \ldots, A_{n-1}) = 0$. La minimalité nous donne tout de suite que $g_0(X_1, \ldots, X_{n-1}) \neq 0$. Noter $A_0 = (-1)^n \cdot t_1 t_2 \cdots t_n$. Prenons $t_n = 0$ partout (c'est-à-dire, nous évaluons tous les polynômes pour $t_n = 0$ sans changer les autres variables). On trouve $A_0 = 0$. En conséquence

$$g_0(A_1, \ldots, A_{n-1}) = 0.$$

Comme nous avons (toujours pour $t_n = 0$)

$$f(X) = X \cdot \prod_{i=1}^{n-1}(X - t_i) = X \cdot (\sum_{i=1}^{n-1} A_i X^{i-1} + X^{n-1}),$$

on voit que A_i pour $t_n = 0$ et $1 \leq i \leq n-1$ est « le A_{i-1} » pour les $n-1$ variables $t_1, \ldots, t_{n-1}$. Par l'hypothèse de récurrence, on voit donc $g_0(X_1, \ldots, X_{n-1}) = 0$, contradiction.
(c) Le corps N est généré au dessus de $K(A_1, \ldots, A_n)$ (en fait, même au dessus de K) par les racines $t_1, \ldots, t_n$ du polynôme f. En plus, les $t_1, \ldots, t_n$ sont algébriques sur $K(A_1, \ldots, A_n)$ car ils sont annulés par f. Donc N est un corps de décomposition de f sur $K(A_1, \ldots, A_n)$. Par un exercice, le degré $[N : K(A_1, \ldots, A_n)]$ est un diviseur de $\#S_n = n!$. Puisque $[N : L] = n!$ et $K(A_1, \ldots, A_n) \subseteq L$, il en suit $K(A_1, \ldots, A_n) = L$.
(d) Clair. □

La proposition dit alors que le groupe de Galois du polynôme général de degré n sur un corps K est isomorphe à S_n.

Corollaire 13.14 (Abel)**.** *Soit K un corps parfait. L'équation générale de degré n sur K est résoluble par radicaux si et seulement si $n \leq 4$.*

Démonstration. Les cas $n \leq 4$ sont bien connus. La proposition 13.13 nous dit que le groupe de Galois du corps de décomposition du polynôme général de degré n est isomorphe à S_n. Si $n \geq 5$, le corollaire 13.11 implique donc que f n'est pas résoluble par radicaux. □

Donc pour $n \geq 5$ il n'existe pas de formule pour exprimer les solutions de l'équation générale de degré n en utilisant uniquement $+, -, \cdot, /, \sqrt[\bullet]{\bullet}$.

14 Constructions à la règle et au compas – n-gons réguliers

Objectifs :

- Connaître la définition des nombres premiers de Fermat ;
- connaître les extensions cyclotomiques de $\mathbb{Q}$ et leurs propriétés fondamentales ;
- connaître le résultat principal sur la constructibilité du n-gon régulier par règle et compas et l'idée fondamentale de sa démonstration,
- connaître des exemples et savoir démontrer des propriétés simples.

On commence cette section par une excursion sur les corps cyclotomiques. Nous avons déjà rencontré des extensions cyclotomiques plus tôt. Maintenant nous allons nous concentrer sur les extensions cyclotomiques de $\mathbb{Q}$ et obtenir des informations dans le contexte de la théorie de Galois.

Proposition 14.1. *Soit $n \in \mathbb{N}$. Soit μ_n le sous-groupe de $\mathbb{C}^\times$ (pour la multiplication) qui est composé de tous les éléments de $\mathbb{C}^\times$ dont l'ordre divise n. On pose $\zeta_n = e^{2\pi i/n} \in \mathbb{C}^\times$. Soit $K = \mathbb{Q}(\zeta_n)$ la n-ème extension cyclotomique de $\mathbb{Q}$.*

(a) K est le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$ et $K/\mathbb{Q}$ est une extension galoisienne finie.

(b) L'application $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ donnée par $j \mapsto \zeta_n^j$ est un isomorphisme de groupes (pour l'addition de $\mathbb{Z}/n\mathbb{Z}$).

(c) Les deux assertions suivantes sont équivalentes :

(i) L'ordre de ζ_n^j dans $\mu(n)$ est égal à n. (On appelle un tel ζ_n^j une n-ième racine primitive *de l'unité.)*

(ii) $j \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(d) On pose $\Phi_n(X) = \prod_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^j) \in \mathbb{C}[X]$. On a $\Phi_n(X) \in \mathbb{Q}[X]$.

(e) On a la factorisation $X^n - 1 = \prod_{d|n, d>0} \Phi_d(X)$ où d parcourt les diviseurs positifs de n.

(f) $\Phi_n(X) \in \mathbb{Z}[X]$ est le polynôme minimal de ζ_n sur $\mathbb{Q}$.

*(g) L'application, appelée n-*ème caractère cyclotomique*,*

$$\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

donnée par la règle $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$ est un isomorphisme de groupes.

Démonstration. (a) Les éléments de μ_n sont précisement les racines de $X^n - 1$. On a $\zeta_n \in \mu_n$ et $\mu_n = \{\zeta_n^j \mid j = 0, \ldots, n-1\}$. Donc le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$ est égal à $\mathbb{Q}(\mu_n)$ et on a l'égalité $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$.
(b) est clair.

(c) Par (b), il suffit de trouver les éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre n. Pour $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ et $r \in \mathbb{N}$, on a $r\overline{a} = \overline{ra} = \overline{0}$ si et seulement si $n \mid ra$. Si $\mathrm{pgcd}(a,n) = 1$, alors cela est le cas si et seulement si $n \mid r$ (donc si l'ordre est n). Si $1 < s = \mathrm{pgcd}(a,n)$, alors $n = s \cdot \frac{n}{s}$ et l'ordre est strictement inférieur à n.
(d) Soit $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Comme σ est un isomorphisme, on a $\sigma((\zeta_n^j)^i) = \sigma((\zeta_n)^j)^i$. Alors ζ_n^j est d'ordre n si et seulement si $\sigma(\zeta_n^j)$ est d'ordre n. En conséquence, σ permute l'ensemble $\{\zeta_n^j \mid j \in (\mathbb{Z}/n\mathbb{Z})^\times\}$.
Ici, nous pouvons déjà affirmer que χ est une application bien définie. Elle est injective car σ est uniquement déterminée par son image sur les générateurs de K sur $\mathbb{Q}$.
On obtient aussi que $\Phi_n^\sigma(X) = \Phi_n(X)$ (où $\Phi_n^\sigma(X)$ est le polynôme obtenu de $\Phi_n(X)$ en faisant agir σ sur les coefficients). En conséquence, les coefficients de $\Phi_n(X) \in K[X]$ sont invariants par $\mathrm{Gal}(K/\mathbb{Q})$, donc appartiennent à $\mathbb{Q}$.
(e) C'est clair, car l'ordre de ζ_n^j est un diviseur d de n, et ζ_n^j est donc une racine de Φ_d.
(f) On a $\Phi_n(X) \in \mathbb{Z}[X]$ par récurrence et le corollaire 6.5.
Pour voir l'irréductibilité de Φ_n, on suppose $\Phi_n(X) = f(X) \cdot g(X)$ pour $f, g \in \mathbb{Z}[X]$ unitaires et f le polynôme minimal de ζ_n^j sur $\mathbb{Q}$ pour un $j \in (\mathbb{Z}/n\mathbb{Z})^\times$. On considère un nombre premier p qui ne divise pas n. On montre $f(\zeta_n^{jp}) = 0$. Supposons que cela n'est pas le cas. Alors $g(\zeta_n^{jp}) = 0$. Donc ζ_n^j est un zéro du polynôme $h(X) := g(X^p)$; en conséquence, $f \mid h$. Considérons maintenant les réductions modulo p des polynômes f, g, h, notées $\overline{f}, \overline{g}, \overline{h} \in \mathbb{F}_p[X]$. Comme pour tout polynôme dans $\mathbb{F}_p[X]$, on a $(\overline{g}(X))^p = \overline{g}(X^p) = \overline{h}(X)$, il en suit que $\overline{f}$ divise $(\overline{g}(X))^p$, d'où $\mathrm{pgcd}(\overline{f}, \overline{g}) \not\sim 1$. Par contre, $\overline{f}$ et $\overline{g}$ sont des diviseurs du polynôme $X^n - 1 \in \mathbb{F}_p[X]$. Ce polynôme est séparable car le pgcd de sa dérivée nX^{n-1} et $X^n - 1$ est 1 (comme 0 est la seule racine de nX^{n-1} tandis que 0 n'est pas une racine de $X^n - 1$). Donc $\mathrm{pgcd}(\overline{f}, \overline{g}) \sim 1$. Contradiction.
En rajoutant un nombre premier après l'autre, cela montre que si $f(\zeta_n) = 0$, alors $f(\zeta_n^r) = 0$ pour tout $r \in \mathbb{N}$ tel que $\mathrm{pgcd}(r,n) = 1$. Donc $g(X) = 1$ et $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.
(g) L'application χ est un homomorphisme de groupes : soient $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$; on a

$$\zeta_n^{\chi(\sigma\tau)} = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{\chi(\tau)}) = \sigma(\zeta_n)^{\chi(\tau)} = (\zeta_n^{\chi(\sigma)})^{\chi(\tau)} = \zeta_n^{\chi(\sigma)\chi(\tau)}.$$

Cette application est surjective car pour tout $j \in (\mathbb{Z}/n\mathbb{Z})^\times$ il existe un $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $\sigma(\zeta_n) = \zeta_n^j$ car les deux sont des racines du polynôme minimal Φ_n de ζ_n sur $\mathbb{Q}$. □

Il nous faut encore un petit résultat en théorie des groupes.

Proposition 14.2. *Soit G un groupe abélien fini de cardinal $m > 1$. Alors :*

(a) Il existe un élément $g \in G$ d'ordre un nombre premier $p \mid m$.

(b) Il existe $n \in \mathbb{N}$ et des sous-groupes normaux

$$\{1\} = G_n \lhd G_{n-1} \lhd G_{n-2} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

tels que G_{i-1}/G_i est cyclique d'ordre un nombre premier qui divise m.

Démonstration. (a) Soit $1 \neq h \in G$ n'importe quel élément de G. Son ordre divise le cardinal du groupe. Soit p un nombre premier qui divise $\mathrm{ord}(h)$ (et donc m). Écrivons $\mathrm{ord}(h) = pq$. Donc l'ordre de $g := h^q$ est égal à p.

(b) Remarquons d'abord que tout sous-groupe est normal car G est abélien. Soit n le nombre des nombres premiers qui apparaissent dans la factorisation de m. On pose $G_n := \{1\}$. Pour $i = 0, \dots, n-1$, nous procédons récursivement. Par (a), il existe $g_i \in G$ tel que son image $g_i G_{n-i}$ dans G/G_{n-i} est d'ordre un nombre premier p_i divisant m. On pose $G_{n-i-1} := \langle g_0, \dots, g_i \rangle$. On a $G_{n-i-1}/G_{n-i} = \langle g_i G_{n-i} \rangle$ est de cardinal p_i. En plus, le cardinal de G_{n-i-1} est le produit des nombres premiers $p_0 p_1 \dots p_i$, donc $G_0 \subseteq G$ est d'ordre $p_0 \dots p_{n-1} = m$, d'où $G_0 = G$. □

Définition-Lemme 14.3. *Soit $n \in \mathbb{N}$. Si $2^n + 1$ est un nombre premier, alors n est une puissance de 2. On appelle* nombre premier de Fermat *tout nombre premier de la forme $2^{2^r} + 1$.*

Démonstration. Soient $r, s \in \mathbb{N}$ tels que $2^r s \geq 1$ et s est impair. On fait le calcul

$$2^{2^r s} + 1 = (2^{2^r})^s - (-1)^s = (2^{2^r} - (-1)) \cdot (2^{2^r(s-1)} - 2^{2^r(s-2)} + \dots - 2^{2^r} + 1).$$

Cela montre que $2^{2^r} + 1$ divise $2^{2^r s} + 1$. Si $2^{2^r s} + 1$ est premier, comme $2^{2^r} + 1 > 1$, il est nécessaire que $2^{2^r s} + 1 = 2^{2^r} + 1$, donc $s = 1$. □

Les seuls nombres premiers de Fermat connus sont $3 = 2^{2^0} + 1$, $17 = 2^{2^2} + 1$, $257 = 2^{2^3} + 1$ et $65537 = 2^{2^4} + 1$. Euler a été le premier à trouver la factorisation $4294967297 = 2^{2^5} + 1 = 641 \cdot 6700417$.

Théorème 14.4 (Gauß)**.** *Soit $n \in \mathbb{N}_{\geq 3}$. Les assertions suivantes sont équivalentes :*

(i) Etant donné deux points C et P, le n-gon régulier de centre C ayant P comme un des sommets est constructible à la règle et au compas.

(ii) $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ est une puissance de 2.

(iii) Il existe des nombres premiers de Fermat distincts $p_1, \dots, p_s$ et $m \in \mathbb{N}$ tels que

$$n = 2^m p_1 p_2 \cdots p_s.$$

Démonstration. Sans perte de généralité nous pouvons prendre $C = 0$ et $P = 1$. La construction de l'n-gon régulier est équivalente à la construction d'un deuxième sommet, donc à $\zeta_n = e^{2\pi i/n}$ (on obtient les autres par des réflexions). Par la proposition 14.1 on a $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, donc $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$.
« (i) ⇒ (ii) » : Le corollaire 9.8 du théorème principal sur la constructibilité à la règle et au compas montre que le degré $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ doit être une puissance de 2.
« (ii) ⇒ (i) » : Par le théorème principal sur la constructibilité à la règle et au compas (théorème 9.7) il suffit de montrer qu'il existe des corps

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_r$$

tels que $\zeta_n \in L_r$ et $[L_i : L_{i-1}] = 2$ pour tout $1 \leq i \leq r$. Nous avons que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est un groupe fini abélien d'ordre 2^r pour un $r \in \mathbb{N}$. La proposition 14.2 montre l'existence de sous-groupes

$$\{1\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

tels que $(G_i : G_{i-1}) = 2$ pour $1 \leq i \leq r$. La correspondance du théorème principal de la théorie de Galois 12.9 le traduit en la suite de corps recherchée.
« (ii) $\Rightarrow$ (iii) » : Soit $n = 2^m p_1^{e_1} \cdot \cdots \cdot p_s^{e_s}$ la factorisation de n en nombres premiers distincts. Par des formules dérivées dans « structures mathématiques », nous avons $\varphi(n) = 2^{m-1}(p_1 - 1)p_1^{e_1-1} \cdot \cdots \cdot (p_s - 1)p_s^{e_s-1} = 2^r$. Donc $e_1 = e_2 = \cdots = e_s = 1$ et $p_i - 1$ est une puissance de 2 pour tout $1 \leq i \leq s$. Par la définition-lemme 14.3, p_i est un nombre premier de Fermat pour tout $1 \leq i \leq s$.
« (iii) $\Rightarrow$ (ii) » : Nous avons $\varphi(n) = 2^{m-1}(p_1 - 1) \cdot \cdots \cdot (p_s - 1)$ qui est une puissance de 2. □

Remarque 14.5. *Dans le théorème 14.4 on peut remplacer (i) par :*

(i') Etant donné deux points P_1, P_2 du plan, un n-gon régulier dont un côté est le segment $\overline{P_1\ P_2}$ est constructible à la règle et au compas.

La raison est la suivante :
Admettons (i) : Alors, il est possible de construire l'angle $\frac{2\pi}{n}$; donc, il est possible de construire l'angle $\frac{n-2}{n}\pi$; c'est l'angle entre deux côtés voisins du n-gon. Donc, il est possible de contruire le n-gon ayant $\overline{P_1\ P_2}$ comme un de ses côtés.
Admettons (i') : Si on a le n-gon régulier, il est facile de construire son centre. Ayant son centre, on a l'angle $\frac{2\pi}{n}$. A l'aide de cet angle on peut construire les n-gon réguliers avec le centre et un des sommets donnés.

15 Complément : Quelques groupes de Galois

Définition 15.1. *Soient K un corps et $\overline{K}$ une clôture algébrique de K. Soient $f \in K[X]$ un polynôme et $a_1, \ldots, a_n \in \overline{K}$ ses racines.*
On pose

$$\Delta_f := \prod_{1 \leq i < j \leq n} (a_i - a_j)^2$$

et on l'appelle le discriminant de f.

Exemple 15.2. *Soit K un corps.*

(a) Pour $f(X) = X^2 + aX + b$ on a $\Delta_f = a^2 - 4b$.
En effet, $f(X) = (X - a_1)(X - a_2) = X^2 - (a_1 + a_2)X + a_1a_2$ implique

$$(a_1 - a_2)^2 = a_1^2 + a_2^2 - 2a_1a_2 = (a_1 + a_2)^2 - 4a_1a_2 = a^2 - 4b.$$

(b) Pour $f(X) = X^3 + aX + b$ on a $\Delta_f = -4a^3 - 27b^2$.
Cela peut être vérifié par un caclul direct.

Lemme 15.3. *Soient K un corps et $f \in K[X]$.*

(a) f est séparable $\Leftrightarrow \Delta_f \neq 0$.

(b) $\Delta_f \in K$.

Démonstration. (a) C'est clair.
(b) On peut supposer f séparable (car $0 \in K$). Soit L/K un corps de décomposition de f sur K. Donc L/K est une extension galoisienne finie. Ses éléments permutent les racines de f. Donc tout $\sigma \in \mathrm{Gal}(L/K)$ laisse invariant Δ_f. Donc $\Delta_f \in L^{\mathrm{Gal}(L/K)} = K$ par la théorie de Galois. □

Proposition 15.4. *Soient K un corps et $f \in K[X]$ un polynôme séparable. Soit N/K un corps de décomposition de f sur K. C'est une extension galoisienne de K. On dit souvent que* $\mathrm{Gal}(N/K)$ *est* le groupe de Galois de f, *noté* $\mathrm{Gal}(f)$. *Soient $a_1, \ldots, a_n \in N$ les racines de f.*

(a) L'application

$$\varphi : \mathrm{Gal}(N/K) \to S_n, \quad \sigma \mapsto \varphi(\sigma) \text{ où } \sigma(a_i) = a_{\varphi(\sigma)(i)}$$

est un homomorphisme de groupes injectif.

(b) Si $\mathrm{car}(K) \neq 2$, *les assertions suivantes sont équivalentes :*

(i) $\exists\, y \in K$ *tel que* $y^2 = \Delta_f$.
(ii) $\varphi(\mathrm{Gal}\,/N/K)) \subseteq A_n$.

Démonstration. (a) On vérifie l'homomorphie. Soient $\sigma, \tau \in \mathrm{Gal}(N/K)$. On a pour $i = 1, \ldots, n$:

$$a_{\varphi(\sigma\circ\tau)(i)} = \sigma \circ \tau(a_i) = \sigma(\tau(a_i)) = \sigma(a_{\varphi(\tau)(i)}) = a_{\varphi(\sigma)\circ\varphi(\tau)(i)},$$

d'où $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$. Si $\varphi(\sigma) = \mathrm{id}$, on trouve que σ est l'identité sur tout a_i, donc sur les générateurs de N/K, donc σ est l'identité et φ est injectif.
(b) On écrit $\delta = \prod_{1\le i<j\le n}(a_i - a_j)$ et on calcule pour $\sigma \in \mathrm{Gal}(N/K)$:

$$\begin{aligned}
\sigma(\delta) = \sigma(\prod_{1\le i<j\le n}(a_i - a_j)) &= \prod_{1\le i<j\le n}(\sigma(a_i) - \sigma(a_j)) \\
&= \prod_{1\le i<j\le n}(a_{\varphi(\sigma)(i)} - a_{\varphi(\sigma)(j)}) \\
&= \prod_{1\le i<j\le n}\frac{a_{\varphi(\sigma)(i)} - a_{\varphi(\sigma)(j)}}{a_i - a_j}\cdot(a_i - a_j) \\
&= \prod_{1\le i<j\le n}\frac{a_{\varphi(\sigma)(i)} - a_{\varphi(\sigma)(j)}}{a_i - a_j}\cdot\prod_{1\le i<j\le n}(a_i - a_j) \\
&= \prod_{1\le i<j\le n}\frac{\varphi(\sigma)(i) - \varphi(\sigma)(j)}{i - j}\cdot\prod_{1\le i<j\le n}(a_i - a_j) \\
&= \mathrm{sgn}(\varphi(\sigma))\cdot\delta.
\end{aligned}$$

L'assertion (i) est équivalente à $\delta \in K$. Donc (i) est équivalent à $\delta = \sigma(\delta) = \mathrm{sgn}(\varphi(\sigma))\delta$, ce qui équivaut $\mathrm{sgn}(\varphi(\sigma)) = 1$ et $\varphi(\sigma) \in A_n$. □

Corollaire 15.5. *Soit K un corps de caractéristique différent de 2 et soit $f(X) = X^3 + aX + b \in K[X]$ un polynôme irréductible. Alors :*

$$\mathrm{Gal}(f) \cong \begin{cases} A_3 & \text{si } \Delta_f = -4a^3 - 27b^2 \text{ est un carré dans } K \\ S_3 & \text{sinon.} \end{cases}$$

Démonstration. Par la proposition 15.4(a), $\mathrm{Gal}(f)$ est un sous-groupe de S_3. En plus, le fait que f est irréductible implique que tout corps de rupture de f est de degré 3, donc $3 \mid \#\,\mathrm{Gal}(f)$. Mais, S_3 ne possède qu'un seul sous-groupe de cardinal 3, le groupe alterné A_3. Donc, $\mathrm{Gal}(f) \in \{A_3, S_3\}$. Le résultat suit de 15.4(b). □

Exemple 15.6. *(a) On a* $\mathrm{Gal}(f) \cong S_3$ *pour le polynôme* $f(X) = X^3 - X + 1 \in \mathbb{Q}[X]$ *car son discriminant* $\Delta_f = 4 - 27 = -23$ *n'est pas un carré dans* $\mathbb{Q}$.

(b) On a $\mathrm{Gal}(f) \cong A_3$ *pour le polynôme* $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$ *car son discriminant* $\Delta_f = 4 \cdot 27 - 27 = 3 \cdot 27 = 81 = 9^2$ *est un carré dans* $\mathbb{Q}$.

16 Complément : Bases de transcendance

Définition 16.1. *Soit L/K une extension de corps. On appelle* base de transcendance de L/K *tout sous-ensemble $B \subset L$ tel que*

- *tout $x \in B$ est transcendant sur $K(B \setminus \{x\})$,*
- *$L/K(B)$ est une extension algébrique.*

Proposition 16.2. *Toute extension de corps L/K possède une base de transcendance.*

Démonstration. On n'inclut pas la démonstration de cette proposition qui est basée sur le lemme de Zorn. □

Lemme 16.3. *Soit L/K une extension de corps et soit $x \in L$ tel que $L/K(x)$ est algébrique. Alors pour tout $y \in L$ qui est transcendant sur K, l'extension $L/K(y)$ est algébrique.*

Démonstration. Par hypothèse, il existe un polynôme $0 \neq f_x(Y) = \sum_{i=0}^{d} a_i(x)Y^i \in K(x)[Y]$ tel que $f_x(y) = 0$. Ici, les coefficients s'écrivent comme $a_i(x) = \frac{b_i(x)}{c_i(x)}$ pour des polynômes $b_i, c_i \in K[x]$ où $c_i(x) \neq 0$. Si on multiplie f_x par $c_0(x) \cdot c_1(x) \cdots c_d(x)$, on obtient un polynôme $F_x(Y) \in (K[x])[Y]$ tel que $F_x(y) = 0$. Nous interprétons F_x comme élément $F \in K[X, Y]$ tel que $F_x(Y) = F(x, Y)$. Cela nous permet aussi de le lire comme le polynôme $F_y(X) = F(X, y) \in (K(y))[X]$. On a $F_y(x) = 0$. Cela montre que x est algébrique sur $K(y)$. Comme $L/K(x)$ est algébrique, par la transitivité on a $L/K(x, y)/K(y)$ est algébrique. □

Proposition 16.4. *Soit L/K une extension de corps qui possède une base de transcendance de cardinal fini. Alors, toutes les bases de transcendance de L/K possèdent le même cardinal. On parle du* degré de transcendance.

Démonstration. Pour $n \in \mathbb{N}$, soit $\mathcal{L}_n$ la collection de toutes les extensions de corps possédant une base de transcendance de cardinal n. On démontre l'assertion pour toute extension dans $\mathcal{L}_n$ par récurrence sur n.
Le cas $n = 0$ est celui des extensions algébriques. Dans les extensions algébriques il n'existe aucun élément transcendant (par définition), donc toute base de transcendance doit être vide.
Supposons l'assertion démontrée pour $0, 1, \ldots, n-1$ et prenons une extension $L/K \in \mathcal{L}_n$. Soit $B = \{x_1, \ldots, x_n\}$ une base de transcendance de cardinal n et soit $C = \{y_1, \ldots, y_m\}$ une autre de

cardinal m. Si $m < n$, on obtient une contradiction par l'hypothèse de récurrence. Supposons $m \geq n$. Les éléments $x_2, x_3, \ldots, x_n$ forment une base de transcendance de $L/K(x_1)$.
Donc par l'hypothèse de récurrence, toute base de transcendance de $L/K(x_1)$ est de cardinal $n-1$. Cela veut dire que l'on peut choisir un sous-ensemble C_1 de C de cardinal $n-1$ tel que C_1 est une base de transcendance de $L/K(x_1)$. En effet, si l'on ne pouvait pas enlever un y_i sans perdre que $L/K(x_1)(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_m)$ est algébrique, on aurait une base de transcendance de $L/K(x_1)$ de cardinal $m \geq n > n-1$, donc une contradiction. Ainsi on peut continuer à enlever des éléments de C jusqu'à ce qu'il n'en reste que $n-1$.
On a que $C_1 \cup \{x_1\}$ est une base de transcendance de L/K. Si l'on écrit $E = K(C_1)$, alors $L/E(x_1)$ est algébrique. Par le lemme 16.3, pour n'importe lequel $y \in C \setminus C_1$, $L/E(y)$ est algebrique. Cela veut dire que $C_1 \cup \{y\}$ est une base de transcendance pour L/K, donc $m = n$. □

Le corollaire suivant a été utilisé dans la démonstration de la proposition 13.13.

Corollaire 16.5. *Soit N/K une extension de corps ayant la base de transcendance $\{t_1, \ldots, t_n\}$. Alors l'application*

$$\psi : K[T_1, \ldots, T_n] \to N, \quad T_i \mapsto t_i \text{ pour } i = 1, \ldots, n,$$

et qui est l'identité sur K est un homomorphisme d'anneaux injectif.

Démonstration. Soit $f(T_1, \ldots, T_n) \in \ker(\psi)$. Si $f \neq 0$, son perte de généralité la variable T_n apparaît dans f (sinon, changer la numérotation des variables). Posons $L := K(t_1, \ldots, t_{n-1})$. On trouve que t_n est un zéro de f^ψ (vue comme polynôme à coefficients dans L). Donc t_n est algébrique sur L. En conséquence, $t_1, \ldots, t_{n-1}$ est une base de transcendance de N/K de cardinal inférieur ou égal à $n-1$. Comme cela est impossible par la proposition 16.4, on trouve $f = 0$, et ψ est injectif. □

17 Supplément : Théorie de Kummer

Définition 17.1. *Soient G un group et K un corps. On appelle* caractère de G sur K *tout homomorphisme de groupes $\chi : G \to K^\times$.*

Proposition 17.2. *Soient G un group, K un corps et $\chi_1, \ldots, \chi_n$ des caractères deux-à-deux distincts de G sur K. Alors, en tant qu'éléments dans le K-espace vectoriel $\mathrm{Appl}(G, K) := \{f : G \to K \mid \text{ application }\}$, les $\chi_1, \ldots, \chi_n$ sont K-linéairement indépendants.*

Démonstration. On suppose que l'assertion est fausse. Soit n le minimum tel qu'il existe des caractères distincts $\chi_1, \ldots, \chi_n$. On a $n \geq 2$ car le caractère trivial existe. Supposons donc que nous avons la combinaison K-linéaire non-triviale

$$0 = \sum_{i=1}^{n} a_i \chi_i.$$

On a $a_i \neq 0$ pour tout i à cause de la minimalité de n.
Soit $g \in G$ tel que $\chi_1(g) \neq \chi_2(g)$. Pour tout $h \in G$, on a

$$0 = \sum_{i=1}^{n} a_i \chi_i(gh) = \sum_{i=1}^{n} (a_i \chi_i(g)) \chi(h).$$

Cela implique que nous avons une deuxième combinaison K-linéaire

$$0 = \sum_{i=1}^{n} (a_i \chi_i(g)) \chi_i.$$

On prend la différence entre $\chi_1(g)$ fois la première et la deuxième combinaison K-linéaire :

$$0 = \sum_{i=1}^{n} (a_i(\chi_1(g) - \chi_i(g))\chi_i = \sum_{i=2}^{n} (a_i(\chi_1(g) - \chi_i(g))\chi_i.$$

Cela contredit la minimalité de n. □

Corollaire 17.3. *Soit L/K une extension algébrique. Alors les éléments de $\mathrm{Aut}_K(L)$ sont L-linéairement indépendants dans le L-espace vectoriel $\mathrm{Appl}(L, L)$.*

Démonstration. Supposons que $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}_K(L) \subset \mathrm{Appl}(L, L)$ sont L-linéairement dépendants. Alors les caractères $\sigma_i|_{L^\times} : L^\times \to L^\times$ sont L-linéairement dépendants. Contradiction avec la proposition 17.2. □

Définition 17.4. *Soit L/K une extension de corps finie séparable de degré $[L : K] = [L : K]_s = n$ et soient $\sigma_1, \ldots, \sigma_n$ les K-homomorphismes de L dans une clôture algébrique $\overline{K}$ de K.*
Pour $a \in L$ on définit la trace *de a pour l'extension L/K comme*

$$\mathrm{Tr}_{L/K}(a) := \sum_{i=1}^{n} \sigma_i(a)$$

et la norme *de a pour l'extension L/K comme*

$$\mathrm{Nm}_{L/K}(a) := \prod_{i=1}^{n} \sigma_i(a).$$

Proposition 17.5 (Hilbert's Satz 90)**.** *Soit L/K une extension galoisiennce finie cyclique. Soit $\sigma \in \mathrm{Gal}(L/K)$ tel que $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Pour $b \in L$, les assertions suivantes sont équivalentes :*

(i) $\mathrm{Nm}_{L/K}(b) = 1$.

(ii) $\exists\, a \in L^\times : b = \frac{a}{\sigma(a)}$.

Démonstration. « (ii) ⇒ (i) » : Comme on a $b = \frac{a}{\sigma(a)}$, on obtient $\mathrm{Nm}_{L/K}(b) = \frac{\mathrm{Nm}_{L/K}(a)}{\mathrm{Nm}_{L/K}(\sigma(a))} = 1$.
« (i) ⇒ (ii) » : Soit $n = [L : K]$. Alors par le corollaire 17.3, $\mathrm{id} = \sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ sont L-linéairement indépendants dans $\mathrm{Appl}(L, L)$. En particulier, on a

$$0 \neq \mathrm{id} + b\sigma + b\sigma(b)\sigma^2 + \cdots + b\sigma(b)\ldots\sigma^{n-2}(b)\sigma^{n-1}.$$

Il existe donc $c \in L^\times$ tel que

$$0 \neq c + b\sigma(c) + b\sigma(b)\sigma^2(c) + \cdots + b\sigma(b)\ldots\sigma^{n-2}(b)\sigma^{n-1}(c) =: a.$$

On calcule

$$\begin{aligned}\frac{a}{\sigma(a)} &= \frac{c + b\sigma(c) + b\sigma(b)\sigma^2(c) + \cdots + b\sigma(b)\ldots\sigma^{n-2}(b)\sigma^{n-1}(c)}{\sigma(c) + \sigma(b)\sigma^2(c) + \sigma(b)\sigma^2(b)\sigma^3(c) + \cdots + \sigma(b)\sigma^2(b)\ldots\sigma^{n-1}(b)c} \\ &= b\frac{c/b + \sigma(c) + \sigma(b)\sigma^2(c) + \cdots + \sigma(b)\ldots\sigma^{n-2}(b)\sigma^{n-1}(c)}{\sigma(c) + \sigma(b)\sigma^2(c) + \sigma(b)\sigma^2(b)\sigma^3(c) + \cdots + c/b} = b,\end{aligned}$$

où on a utilisé $\sigma(b)\sigma^2(b)\ldots\sigma^{n-1}(b) = \mathrm{Nm}_{L/K}(b)/b = 1/b$. □

Proposition 17.6 (Théorie de Kummer)**.** *Soient K un corps et $n \in \mathbb{N}$ tel que $\mathrm{car}(K) = 0$ ou $\mathrm{car}(K) \nmid n$. On suppose que K contient une n-ème racine de l'unité primitive ζ. Soit L/K une extension galoisienne cyclique de degré n. Alors il existe $a \in L$ tel que $L = K(a)$ et $a^n = c \in K$.*

Démonstration. Comme $\zeta \in K$, on a $\mathrm{Nm}_{L/K}(\zeta) = \zeta^n = 1$. Soit σ un générateur de $\mathrm{Gal}(L/K)$. Par la proposition 17.5, il existe $a \in L$ tel que $\zeta = \frac{a}{\sigma(a)}$, ou bien $\sigma(a) = \zeta^{-1}a$, et en conséquence $\sigma^i(a) = \zeta^{-i}a$ pour tout $i \in \mathbb{Z}$. Donc $a, \sigma(a), \sigma^2(a), \ldots, \sigma^{n-1}(a)$ sont distincts. Donc $\#\mathrm{Hom}_K(K(a), L) \geq n$, alors $n = [L : K] \geq [K(a) : K] \geq [K(a) : K]_s \geq n$, d'où $L = K(a)$. En plus, $\sigma(a^n) = \sigma(a)^n = (\zeta^{-1}a)^n = a^n =: c$. Il en suit $c \in L^{\mathrm{Gal}(L/K)} = K$. □

Lemme 17.7. *Soit G un groupe fini résoluble. Alors, il existe une suite de sous-groupes*

$$G_n = \{1\} \leq G_{n-1} \leq G_{n-2} \leq \cdots \leq G_1 \leq G_0 = G$$

telle que

- *pour tout $1 \leq i \leq n$ on a $G_i \lhd G_{i-1}$ (sous-groupe normal) et*
- *G_{i-1}/G_i est un groupe cyclique (dans la définition 13.5 on n'éxige que « abélien »).*

Démonstration. Par définition, il existe une suite de sous-groupes

$$G_m = \{1\} \leq G_{m-1} \leq G_{m-2} \leq \cdots \leq G_1 \leq G_0 = G$$

telle que $G_{i+1} \trianglelefteq G_i$ et $\overline{G_i} := G_i/G_{i+1}$ est abélien pour tout $i = 0, \ldots, m-1$. Comme $\overline{G}_i$ on peut appliquer la proposition 14.2 pour obtenir une suite de sous-groupes

$$\overline{G}_{i,m_i} = \{1\} \leq \overline{G}_{i,m_i-1} \leq \overline{G}_{i,m_i-2} \leq \cdots \leq \overline{G}_{i,1} \leq \overline{G}_{i,0} = \overline{G_i}$$

telle que $\overline{G}_{i,j}/\overline{G}_{i,j+1}$ est cyclique pour tout $j = 0, \ldots, m_i - 1$. Soit $\pi_i : G_i \to \overline{G}_i = G_i/G_{i+1}$ la projection naturelle. Pour i, j, on pose $G_{i,j} := \pi_i^{-1}(\overline{G}_{i,j})$. Par un théorème d'isomorphisme nous avons $\overline{G}_{i,j}/\overline{G}_{i,j+1} \cong G_{i,j}/G_{i,j+1}$, c'est donc un groupe cyclique. En tout, nous avons la suite

$$G_m = \{1\} \leq G_{m-1,m_{m-1}} \leq G_{m-1,m_{m-2}} \leq \cdots \leq G_{0,2} \leq G_{0,1} \leq G_{0,0} = G_0 = G,$$

comme demandé. □

Nous pouvons maintenant établir que l'implication dans le théorème 13.6 est une équivalence en caractéristique 0.

Théorème 17.8. *Soit K un corps de caractéristique 0 parfait et L/K une extension finie. Alors, les assertions suivantes sont équivalentes :*

(i) L/K est résoluble par radicaux.

(ii) Il existe une extension finie et galoisienne N/K telle que $L \subseteq N$ et le groupe de Galois $\mathrm{Gal}(N/K)$ est résoluble.

Démonstration. « (i) $\Rightarrow$ (ii) » : Théorème 13.6.
« (ii) $\Rightarrow$ (i) » : Soit $n = [N : k]$. Par le lemme 17.7, l existe une suite de sous-groupes

$$G_r = \{1\} \leq G_{r-1} \leq G_{r-2} \leq \cdots \leq G_1 \leq G_0 = G$$

telle que $G_{i+1} \lhd G_i$ est un sous-groupe normal et le quotient G_i/G_{i+1} est cyclique. On pose $N_i := N^{G_i}$. Par le théorème principal de la théorie de Galois, on a la suite d'extensions de corps

$$N = N_r \supseteq N_{r-1} \supseteq N_{r-2} \supseteq \cdots \supseteq N_1 \supseteq N_0 = N^G = K$$

telle que N_{i+1}/N_i est une extension galoisienne cyclique de groupe de Galois $\mathrm{Gal}(N_{i+1}/N_i) = G_i/G_{i+1}$. Soit $\zeta \in \overline{K}$ (clôture algébrique de K) une n-ème racine de l'unité primitive. On pose $M_i := N_i(\zeta)$. Par la proposition 12.12, on a

$$\mathrm{Gal}(\underbrace{N_{i+1}(\zeta)}_{N_{i+1}N_i(\zeta)}/N_i(\zeta)) \cong \mathrm{Gal}(N_{i+1}/(N_{i+1} \cap N_i(\zeta)) \subseteq \mathrm{Gal}(N_{i+1}/N_i).$$

En tant que sous-groupe d'un groupe cyclique, $\mathrm{Gal}(N_{i+1}(\zeta)/N_i(\zeta))$ est cyclique.
L'extension $M_0 = N_0(\zeta) = K(\zeta)/K$ est cyclotomique ; c'est un corps de décomposition de $X^n - 1$ sur K. Par la théorie de Kummer (proposition 17.6), l'extension M_{i+1}/M_i est engendrée par la n_i-ème racine d'un élément de M_i où $n_i = [M_{i+1} : M_i]$ est un diviseur de n ce qui assure que M_i contient une n_i-ème racine de l'unité primitive (car $\zeta \in M_0 \subseteq M_i$). Comme $L \subseteq N \subseteq M$, on a démontré que L/K est résoluble par radicaux. □

18 Supplément : La classification des groupes abéliens

Corollaire 18.1. *Soit G un groupe cyclique.*

(a) Si $H \leq G$ est un sous-groupe (automatiquement normal car G est abélien), alors le quotient G/H est aussi cyclique.

(b) Tout sous-groupe H de G est aussi cyclique.

Démonstration. Par la classification des groupes cycliques (voir Algèbre 1), nous pouvons supposer $G = \mathbb{Z}$ ou $G = \mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}_{\geq 1}$. Ces cas sont un exercice facile. □

Lemme 18.2. *Soient G un groupe abélien fini et $g, h \in G$.*

(a) Si $\mathrm{pgcd}(\mathrm{ord}(g), \mathrm{ord}(h)) = 1$, *alors* $\mathrm{ord}(gh) = \mathrm{ord}(g)\,\mathrm{ord}(h)$.

(b) Il existe $i, j \in \mathbb{N}$ *tels que* $\mathrm{ord}(g^i h^j) = \mathrm{ppcm}(\mathrm{ord}(g), \mathrm{ord}(h))$.

Démonstration. Dans la démonstration nous utilisons des faits sur les ordres des éléments établis en Algèbre 1.
(a) Soit $m := \mathrm{ord}(gh)$. Donc $g^m h^m = 1$ et par $\langle g \rangle \cap \langle h \rangle = \{1\}$, on a $g^m = h^m = 1$. Il en suit que $\mathrm{ord}(g) \mid m$ et $\mathrm{ord}(h) \mid m$, donc $\mathrm{ord}(g)\,\mathrm{ord}(h) \mid m$ (utilisant encore une fois $\mathrm{pgcd}(\mathrm{ord}(g), \mathrm{ord}(h)) = 1$). Il est clair que $(gh)^{\mathrm{ord}(g)\,\mathrm{ord}(h)} = 1$.
(b) Soient

$$\mathrm{ord}(g) = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} \text{ et } \mathrm{ord}(h) = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

les factorisations en nombres premiers (c'est-à-dire, les $p_1, \ldots, p_k$ sont des nombres premiers distincts), où on les trie de la façon que $m_1 \geq n_1, \ldots, m_s \geq n_s$ et $m_{s+1} < n_s, \ldots, m_k < n_k$. Soient

$$g' := g^{p_{s+1}^{m_{s+1}} \cdot \ldots \cdot p_k^{m_k}} \text{ et } h' := h^{p_1^{n_1} \cdot \ldots \cdot p_s^{n_s}}.$$

Nous avons

$$\mathrm{ord}(g') = p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \text{ et } \mathrm{ord}(h') = p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k}.$$

Donc, (a) implique que l'ordre de $g'h'$ est

$$p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \cdot p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k} = \mathrm{ppcm}(\mathrm{ord}(g), \mathrm{ord}(h)).$$

□

Définition 18.3. *Soit G un groupe. On considère l'ensemble $M := \{n \in \mathbb{N}_{>0} \mid \forall\, g \in G : g^n = 1\}$. Si $M \neq \emptyset$, alors, on définit* l'exposant du groupe *G comme le plus petit élément dans M. Si $M = \emptyset$, on dit que l'exposant du groupe G est infini. Notation :* $\exp(G)$.

Proposition 18.4. *Soit G un groupe abélien fini.*

(a) Il existe $g \in G$ tel que $\mathrm{ord}(g) = \exp(g)$.

(b) $\exp(g) \mid \#G$.

(c) $\exp(G) = \mathrm{ppcm}(\mathrm{ord}(g) \mid g \in G)$.

(d) G est cyclique $\Leftrightarrow \exp(G) = \#G$.

Démonstration. Soit $n := \mathrm{ppcm}(\mathrm{ord}(g) \mid g \in G)$. Il est clair que $g^n = 1$ pour tout $g \in G$, donc $\exp(G) \leq n$. Le lemme 18.2 (b) montre qu'il existe $g \in G$ tel que $\mathrm{ord}(g) = n$. En conséquence $n \leq \exp(G)$. Toutes les assertions sont maintenant claires. □

Sans démonstration on énonce la classification des groupes abéliens de type fini.

Théorème 18.5 (Classification des groupes abéliens de type fini)**.** *Soit G un groupe abélien de type fini (c'est-à-dire que G peut être engendré par un nombre fini d'éléments). Alors, il existe des uniques $r, s \in \mathbb{N}$ et des uniques $d_1, d_2, \ldots, d_s \in \mathbb{N}_{\geq 2}$ tels que*

- $d_1 \mid d_2 \mid \cdots \mid d_s$ *et*
- $G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$.

Exemple 18.6. *On obtient du théorème 18.5 qu'à isomorphisme près il n'existe que deux groupes abéliens de cardinal* 12*, en l'occurence* $\mathbb{Z}/12\mathbb{Z}$ *et* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

19 Supplément : Extensions inséparables

Lemme 19.1. *Soit K un corps de caractéristique $p > 0$, $\overline{K}$ une clôture algébrique de K et $a \in K$. Alors, pour tout $n \in \mathbb{N}$ et pour tout $a \in K$ il existe un et un seul $b \in \overline{K}$ tel que $b^{p^n} = a$.*

Démonstration. Exercice. □

Lemme 19.2. *Soient K un corps de caractéristique $p > 0$, L/K une extension et $\alpha \in L$ algébrique sur K. Alors, les asserions suivantes sont équivalentes :*

(i) *α est séparable sur K.*

(ii) *$K(\alpha) = K(\alpha^p)$.*

Démonstration. Exercice. □

Proposition 19.3. *Soient K un corps de caractéristique $p > 0$, $\overline{K}$ une clôture algébrique de K et $f \in K[X]$ irréductible. Soit $r \in \mathbb{N}$ le maximum tel qu'il existe un polynôme $h \in K[X]$ avec la propriété $f(X) = h(X^{p^r})$. Soit $g \in K[X]$ tel que $g(X^{p^r}) = f(X)$. Alors :*

(a) *g est irréductible et séparable.*

(b) *La multiplicité de toute racine de f est égale à p^r.*

(c) *Les zéros de f dans $\overline{K}$ sont précisement les uniques p^n-ème racines des zéros de g dans $\overline{K}$.*

(d) *Soit $a \in \overline{K}$ un zéro de f. Alors : $[K(a) : K] = p^r[K(a) : K]_s$.*

Démonstration. Exercice. □

Corollaire 19.4. *Soit L/K une extension finie.*

(a) *Si $\mathrm{car}(K) = 0$, alors $[L : K] = [L : K]_s$ et L/K est séparable.*

(b) *Si $\mathrm{car}(K) = p > 0$, alors il existe r tel que $[L : K] = p^r[L : K]_s$.*

Démonstration. Cela suit de la multiplicativité des degrés de corps et de séparabilité. □

Corollaire 19.5. *Soit L/K une extension finie de corps de caractéristique $p > 0$. Si $p \nmid [L : K]$, alors L/K est séparable.*

Démonstration. Cela suit directement du corollaire 19.4. □

Définition 19.6. *Soient K un corps et $\overline{K}$ une clôture algébrique de K.*

(a) *On appelle* purement inséparable *tout polynôme $f \in K[X]$ tel que qu'il possède exactement un zéro dans $\overline{K}$.*

(b) *Soit L/K une extension algébrique. On appelle* purement inséparable *tout $\alpha \in L$ tel que le polynôme minimal de α sur K est purement inséparable.*

(c) On appelle purement inséparable *toute extension algébrique L/K telle que tout $\alpha \in L$ est purement inséparable sur K.*

Lemme 19.7. *Soient K un corps de caractéristique $p > 0$, L/K une extension algébrique et $\alpha \in L$ purement inséparable sur K. Alors, il existe $c \in K$ et $r \in \mathbb{N}$ tel que $f_\alpha(X) = X^{p^r} - c \in K[X]$ est le polynôme minimal de α sur K. En plus, $[K(\alpha) : K]_s = 1$.*

Démonstration. Soit $f_\alpha(X) \in K[X]$ le polynôme minimal de α sur K. Par la proposition 19.3, il existe un polynôme irréductible et séparable $g(X) \in K[X]$ et $r \in \mathbb{N}$ tels que $f_\alpha(X) = g(X^{p^r})$. Comme α est purement inséparable sur K, le polynôme $g(X)$ ne possède qu'un seul zéro (dans une clôture algébrique $\overline{K}$ de K). Donc $g(X) = X - c$ pour un $c \in K$. Comme le degré de séparabilité est égal au nombre de racines (dans une clôture algébrique), la dernière assertion suit aussi. □

Lemme 19.8. *Soit L/K une extension algébrique de corps de caractéristique $p > 0$. Alors les assertions suivantes sont équivalentes :*

(i) L/K est purement inséparable.

(ii) L est engendré sur K par des éléments purement inséparables.

(iii) $[L : K]_s = 1$.

(iv) Pour tout $\alpha \in L$, il exist $r \in \mathbb{N}$ tel que $\alpha^{p^r} \in K$.

Démonstration. « (i) ⇒ (ii) » : On peut prendre L comme ensemble de générateurs.
« (ii) ⇒ (iii) » : Soit $S \subseteq L$ un sous-ensemble qui engendre L sur K tel que les éléments de S sont purement inséparables. On a :

$$L = \bigcup_{T \subseteq S \text{ sous-ensemble fini}} K(T)$$

car tout élément de L peut s'écrire à l'aide d'un nombre fini de générateurs. Soit $T = \{\alpha_1, \ldots, \alpha_n\}$. On utilise la multiplicativité du degré de séparabilité ainsi :

$$\begin{aligned}[K(T) : K]_s =& [K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})]_s \cdot \\ & [K(\alpha_1, \ldots, \alpha_{n-2})(\alpha_{n-1}) : K(\alpha_1, \ldots, \alpha_{n-2})]_s \cdot \ldots \cdot \\ & [K(\alpha_1)(\alpha_2) : K(\alpha_1)]_s \cdot [K(\alpha_1) : K]_s = 1 \cdot \ldots \cdot 1 \cdot 1 = 1\end{aligned}$$

« (iii) ⇒ (iv) » : Soient $\alpha \in L$ et $f_\alpha \in K[X]$ son polynôme minimal sur K. On sait par la proposition 19.3, qu'il existe un polynôme irréductible et séparable $g(X) \in K[X]$ et $r \in \mathbb{N}$ tels que $f_\alpha(X) = g(X^{p^r})$ Par l'hypothèse (iii) et la multiplicativité du degré de séparabilité, $[K(\alpha) : K]_s = 1$. Cela veut dire que g ne possède qu'une seule racine dans $\overline{K}$ (clôture algébriqu de K). Donc $g(X) = X - c$ pour un $c \in K$. En conséquence : $\alpha^{p^r} = c \in K$.
« (iv) ⇒ (i) » : Soit $\alpha \in L$. Nous avons que $X^{p^r} - \alpha^{p^r} = (X - \alpha)^{p^r}$ est un polynôme dans $K[X]$ ayant α comme zéro. Comme le polynôme minimal de α sur K est un diviseur de ce polynôme, il est purement inséparable. Donc L/K est purement inséparable. □

Corollaire 19.9. *Soient $M/L/K$ des extensions algébriques. Alors, M/K est purement inséparable si et seulement si M/L et L/K sont purement inséparables.*

Démonstration. C'est une conséquence directe de la multiplicativité du degré de séparabilité : $[M : K]_s = [M : L]_s \cdot [L : K]_s$. □

Nous allons maintenant trouver, dans toute extension algébrique L/K, un corps intermédiaire E tel que L/E est purement inséparable et E/K est séparable. Ensuite, sous l'hypothèse de la normalité, on saura inverser les deux extensions : L/E séparable et E/K purement inséparable.

Proposition 19.10. *Soit L/K une extension algébrique. On pose*

$$K_s = \{\alpha \in L \mid \alpha \text{ est séparable sur } K\},$$

appelé la clôture séparable de K dans L.

(a) Alors, K_s est l'unique corps tel que $K \subseteq K_s \subseteq L$, L/K_s est purement inséparable et K_s/K est séparable.

(b) $[L : K]_s = [K_s : K] = [K_s : K]_s$.

(c) Si L/K est normal, aussi K_s/K est normal.

Démonstration. (a) D'abord on montre que K_s est un corps, plus précisement, un sous-corps de L. C'est la même preuve que pour montrer que la clôture algébrique d'un corps dans une extension est un corps. Soient $\alpha, \beta \in K_s$. On considère l'extension $K(\alpha, \beta)/K$. Elle est séparable car elle est engendrée par des éléments séparables. Donc $K(\alpha, \beta) \subseteq K_s$. En particulier, $\alpha - \beta, \alpha \cdot \beta, \alpha/\beta \in K_s$ (on considère le dernier seulement si $\beta \neq 0$), montrant que K_s est un corps.
L'extension K_s/K est séparable par définition.
Soient $\alpha \in L$ et $f_\alpha(X) \in K_s[X]$ son polynôme minimal. On montre qu'il est purement inséparable (ce qui implique que L/K_s est purement inséparable). On sait par la proposition 19.3, qu'il existe un polynôme irréductible et séparable $g(X) \in K[X]$ et $r \in \mathbb{N}$ tels que $f_\alpha(X) = g(X^{p^r})$. Donc g est le polynôme minimal sur K de $\alpha^{p^r} := c$. Comme g est séparable, $c \in K_s$. En conséquence, $g(X) = X - c$, d'ou l'inséparabilité de f_α.
Considérons maintenant l'unicité. Soit K' un corps tel que $K \subseteq K' \subseteq L$ et L/K' est purement inséparable et K'/K est séparable. La dernière assertion implique $K' \subseteq K_s$. Si $K_s \neq K'$, alors il existe $\alpha \in K_s \setminus K'$ tel que α est purement inséparable sur K (à cause de la propriété de K') et en même temps α est séparable sur K (à cause de la propriété de K_s) ; cela est une contradiction.
(b) est une conséquence directe de (a) par la multiplicativité du degré de séparabilité et le fait que le degré de séparabilité est égal au degré de l'extension si elle est séparable : $[L : K]_s = [L : K_s]_s \cdot [K_s : K]_s = 1 \cdot [K_s : K]_s = [K_s : K]$.
(c) Soit $\overline{L}$ une clôture algébrique de L. Considérons $\sigma : K_s \to \overline{L}$ un K-homomorphisme. Nous pouvons le prolonger $\tilde{\sigma} : L \to \overline{L}$. A cause de la normalité de L/K, l'image de $\tilde{\sigma}$ appartient à L, et on a un K-isomorphisme $\tilde{\sigma} : L \to L$. Soit $\alpha \in L$. On sait que α et $\tilde{\sigma}(\alpha)$ on le même polynôme minimal sur K. Donc α est séparable sur K si et seulement si $\tilde{\sigma}(\alpha)$ est séparable sur K. Nous pouvons donc conclure $\tilde{\sigma}(K_s) = K_s$, d'où $\sigma(K_s) = K_s$. Cela montre la normalité de K_s/K. □

Proposition 19.11. *Soit L/K une extension algébrique normale. On pose*

$$K_i = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ pour tout } \sigma \in \mathrm{Aut}_K(L)\} = L^{\mathrm{Aut}_K(L)}.$$

Alors, K_i est l'unique corps tel que $K \subseteq K_i \subseteq L$, L/K_i est séparable et K_i/K est purement inséparable.

Démonstration. Si $\mathrm{Aut}_K(L)$ est un groupe fini, on peut abréger la démonstration en utilisant la proposition 12.7. Mais on le fait pas ici.
On montre d'abord que K_i est un corps. Pour cela, soient $\alpha, \beta \in K_i$, donc $\sigma(\alpha) = \alpha$ et $\sigma(\beta) = \beta$ pour tout $\sigma \in \mathrm{Aut}_K(L)$. Cela implique $\sigma(\alpha - \beta) = \alpha - \beta$, $\sigma(\alpha \cdot \beta) = \alpha \cdot \beta$ et $\sigma(\alpha/\beta) = \alpha/\beta$ (la dernière assertion seulement si $\beta \neq 0$), d'où $\alpha - \beta, \alpha \cdot \beta, \alpha/\beta \in K_i$. Donc K_i est un sous-corps de L.
Soit $\sigma : K_i \to L$ un K-homomorphisme (à cause de la normalité il suffit de prendre L comme ensemble d'arrivée). On peut le prolonger à un K-isomorphisme $\tilde{\sigma} : L \to L$. Donc $\sigma \in \mathrm{Aut}_K(L)$. En conséquence, $\tilde{\sigma}|_{K_i} = \mathrm{id}_{K_i}$, donc $\sigma = \mathrm{id}_{K_i}$. Cela montre $[K_i : K]_s = 1$ et l'extension K_i/K est purement inséparable.
Soit $K \subseteq K' \subseteq L$ tel que K'/K est purement inséparable : $[K' : K]_s = 1$, d'où $\mathrm{Hom}_K(K', L) = \{\mathrm{id}_{K'}\}$. En particulier, pour tout $\sigma \in \mathrm{Aut}_K(L)$ on a $\sigma|_{K'} = \mathrm{id}_{K'}$. Cela implique $K' \subseteq K_i$. Le corps K_i contient donc tout sous-corps de L qui est purement inséparable sur K. Dans ce sens, K_i est le sous-corps maximal de L qui est purement inséparable sur K.
Soit $\alpha \in L$. On pose $S = \{\sigma(\alpha) \mid \sigma \in \mathrm{Aut}_K(L)\} \ni \alpha$ et on écrit

$$f(X) = \prod_{s \in S} (X - s) \in L[X].$$

Comme $\mathrm{Aut}_K(L)$ permute les éléments de S, on conclut $f(X) \in L^{\mathrm{Aut}_K(L)}[X] = K_i[X]$. Le polynôme f étant séparable (par construction), montre que α est séparable sur K_i, d'où la séparabilité de L/K_i.
L'unicité suit de la maximalité de K_i ci-dessus. □

20 Supplément : Actions de groupes

On aurait pu (du) inclure cette définition un peu plus tôt.

Définition-Lemme 20.1. *Soit $(G, \star, e)$ un groupe. On pose*

$$\mathrm{Aut}(G) := \{\varphi : G \to G \mid \varphi \text{ est un isomorphisme }\}.$$

Par id_G on note l'identité $G \to G$. Alors, $(\mathrm{Aut}(G), \circ, \mathrm{id}_G)$ est un groupe, appelé groupe des automorphismes de G.

Démonstration. C'est clair ! □

Dans le contexte des actions de groupes (voir ci-dessous), on peut faire agir G sur lui-même. Cela mène au résultat suivant de Cayley.

Proposition 20.2 (Cayley)**.** *Soit $(G, \star, e)$ un groupe fini. Soit $S(G) := \{\sigma : G \to G \mid$ bijection $\}$. Rappelons que $(S(G), \circ, \mathrm{id}_G)$ est le groupe symétrique sur l'ensemble G.*

(a) Pour $g \in G$ on définit une bijection par

$$\sigma_g : G \to G, \quad h \mapsto g \star h.$$

(b) L'application

$$\varphi : G \to S(G), \quad g \mapsto \sigma_g$$

est un homomorphisme de groupes qui est injectif.

Démonstration. (a) On vérifie qu'il s'agit en effet d'une bijection :

Injectivité Si $\sigma_g(h_1) = \sigma_g(h_2)$, alors par définition $g \star h_1 = g \star h_2$ et en conséquence $h_1 = g^{-1} \star g \star h_1 = g^{-1} \star g \star h_2 = h_2$.

Surjectivité Soit $h \in G$. Alors, $\sigma_g(g^{-1} \star h) = g \star g^{-1} \star h = h$, donc nous avons montré que $h \in \mathrm{im}(\varphi)$.

(b) Soit $h \in G$. Alors :

$$\sigma_{g_1} \circ \sigma_{g_2}(h) = \sigma_{g_1}(g_2 \star h) = g_1 \star (g_2 \star h) = (g_1 \star g_2) \star h = \sigma_{g_1 \star g_2}(h).$$

Donc

$$\varphi(g_1) \circ \varphi(g_2) = \sigma_{g_1} \circ \sigma_{g_2} = \sigma_{g_1 \star g_2} = \varphi(g_1 \star g_2),$$

et φ est un homomorphisme de groupes.
Pour l'injectivité prenons g tel que $\sigma_g = \mathrm{id}_G$. Donc on a $\sigma_g(e) = g \star e = g = \mathrm{id}_G(e) = e$. Donc le seul élément dans le noyau de φ est e et on conclut que φ est injectif. □

Groupes de symétries

Définition 20.3. *On appelle* isométrie du plan *toute application*

$$\varphi : \mathbb{R}^2 \to \mathbb{R}^2$$

telle que pour tout $x, y \in \mathbb{R}^2$

$$|\varphi(x) - \varphi(y)| = |x - y|.$$

En d'autres mots, les isométries sont les applications du plan qui préservent les distances.
L'ensemble des isométries du plan est noté I_2. *Noter que* $(I_2, \circ, \mathrm{id})$ *est un groupe.*

Exemple 20.4. *(a) Toute réflexion à un point ou à un axe est une isométrie.*

(b) Toute rotation autour d'un point est une isométrie.

Définition 20.5. *Soit* $F \subset \mathbb{R}^2$ *un sous-ensemble (une figure). On appelle* symétrie de F *toute isométrie* $\varphi \in I_2$ *telle que* $\varphi(F) = F$.
L'ensemble de toutes les symétries de F *est un groupe : le* groupe des symétries de F *:* $\mathrm{Sym}(F)$.

Exemple 20.6. *(au tableau)*

(a) 4 *symétries du losange (sommets nommés A,B,C,D ; angles aigus à* A *et* C*, angles obtus à* B *et* D*) :* id*,* s_x *(réflexion à l'axe* x*),* s_y *(réflexion à l'axe* y*),* $r = s_y \circ s_x = s_y \circ s_x$ *(rotation de* $180°$*).*

(b) $2n$ *symétries du* n*-gone régulier (on numérote les sommets* P_i *à l'inverse du sens des aiguilles d'une montre) :* r^i *pour* $i = 0, \dots, n-1$ *avec* r *la rotation autour* $360°/n$*, et* $s \circ r^i$ *pour* $i = 0, \dots, n-1$ *avec* s *la réflexion à l'axe à travers un sommet et le centre. On a* $s \circ r_i = r_i^{-1} \circ s = r_{n-i} \circ s$*.*

Si n *est pair, on n'a que* $n/2$ *réflexions à l'axe à travers un sommet et le centre. Par contre, il existe aussi* $n/2$ *réflexions à des axes à travers le centre qui sont perpendiculaires à un côté (automatiquement à deux côtés). On se convainc que quand-même toute réflexion est de la forme* sr^i*.*

Lemme 20.7. *L'ensemble* $V = \{\mathrm{id}, s_x, s_y, r\}$ *est l'ensemble de toutes les symétries du losange. Donc* V *est le groupe des symétries du losange.*

Démonstration. Soit σ une symétrie du losange. Soit, σ garde l'angle aigu (autour de A) invariant, soit σ le transforme à l'autre angle aigu (autour de C). Dans le premier cas, on pose $\tau = \sigma$, dans le deuxième cas on pose $\tau = r_y \circ \sigma$. Maintenant, $\tau(A) = A$, donc $\tau(C) = C$. Soit τ garde l'angle obtu (autour de B) invariant, soit τ le transforme en l'autre angle obtu (autour de D). Dans le premier cas, on pose $\rho = \tau$, dans le deuxième cas on pose $\rho = r_x \circ \tau$. On a maintenant que $\rho(A) = A$, $\rho(B) = B$, $\rho(C) = C$, $\rho(D) = D$. Donc $\rho = \mathrm{id}$. □

Lemme 20.8. *L'ensemble* $D_n = \{r^i \mid i = 0, \dots, n-1\} \cup \{sr^i \mid i = 0, \dots, n-1\}$ *est l'ensemble de toutes les symétries du* n*-gone régulier. Donc* D_n *est le groupe des symétries du* n*-gone régulier. Son cardinal est* $2n$*.*

Démonstration. On remarque d'abord que toute symétrie préserve la propriété que deux sommets sont voisins. On note aussi que la réflexion r inverse la numérotation : si avant la réflexion, la numérotation était dans le sense des aiguilles d'une montre, après la numérotation sera dans le sens inverse, et vice versa.
Soit σ une symétrie. Comme σ transforme sommets voisins en sommets voisins, soit σ préserve l'ordre de la numérotation, soit σ l'inverse. Dans le premier cas, on pose $\tau = \sigma$, dans le deuxième cas on pose $\tau = s \circ \sigma$. Maintenant τ préserve l'ordre de la numérotation. Donc après une rotation r_i convenable, $r_i \circ \tau$ est l'identité sur l'ensemble des sommets, donc $r_i \circ \tau = \mathrm{id}$. Cela montre que σ est soit une rotation, soit une rotation suivie par la réflexion. □

Actions de groupes

Toute symétrie du n-gone régulier envoie un sommet sur un sommet et elle est uniquement déterminée par ce qu'elle fait avec les sommets. Cela mène au concept de l'action d'un groupe sur un ensemble.
Pour être plus concret, considérons l'exemple du pentagone (5-gone) régulier. Numérotons les sommets A, B, C, D, E à l'inverse du sens des aiguilles d'une montre. Soit $E = \{A, B, C, D, E\}$ l'ensemble des sommets. Toute symétrie est donc une application bijective de E dans E. En d'autres mots, toute symétrie du 5-gon est un élément du groupe symétrique S_E. Si on appelle les sommets $1, 2, 3, 4, 5$, alors le groupe des symétries du 5-gon est un sous-groupe de S_5. La rotation autour du centre par $72°$ correspond au cycle $(1\ 2\ 3\ 4\ 5)$ et la réflexion à l'axe à travers le centre et 1 est la permutation $(2\ 5)(3\ 4)$.

Définition 20.9. *Soient E un ensemble et G un groupe. On dit que G* agit (à gauche) *sur E (on parle d'une* action (ou opération) du groupe sur l'ensemble *E) s'il existe une application*

$$G \times E \to E, \quad (g, x) \mapsto g.x = gx$$

telle que

- $\forall\, g, h \in G \forall\, x \in E : g.(h.x) = (gh).x$ *et*
- $\forall x \in E : 1.x = x$.

Les opérations à droite peuvent êtres définies d'une manière similaire.

Exemple 20.10. *(a) Le groupe des symétries d'un n-gone régulier agit sur l'ensemble des sommets.*

(b) Soit G un groupe et $E = G$. Nous prenons la loi de groupe $G \times E \to E$, $(g, e) \mapsto g \cdot e$ pour définir une action à gauche de G sur lui-même.

(c) Soit G un groupe et encore $E = G$. La conjugaison *$G \times E \to E, (g, e) \mapsto geg^{-1}$ définit une action à gauche de G sur lui-même. (La seule chose non-triviale à vérifier, c'est $(gh)e(gh)^{-1} = g(heh^{-1})g^{-1}$.)*

Toute opération d'un groupe sur un ensemble peut être exprimée dans le groupe symétrique. Plus précisément, nous avons les assertions suivantes.

Lemme 20.11. *Soient G un groupe et E un ensemble.*

(a) Si $G \times E \to E$ est une opération de groupe, l'application $\varphi : G \to S_E$ donnée par la règle que $\varphi(g)$ est l'application $E \to E$ telle que $(\varphi(g))(e) = g.e$ est un homomorphisme de groupes.

(b) Si $\varphi : G \to S_E$ est un homorphisme de groupes, alors $g.e := (\varphi(g))(e)$ définit une opération à gauche de G sur E.

(c) Les constructions de (a) et (b) établissent une bijection entre l'ensemble des homomorphismes de groupes $G \to S_E$ et les opérations à gauche de G sur E.

Démonstration. (a) D'abord il faut vérifier que $\varphi(g)$ est une bijection $E \to E$. Si $(\varphi(g))(x) = (\varphi(g))(y)$ avec $x, y \in E$, alors on a $g.x = g.y$; en agissant par g^{-1}, on obtient $g^{-1}.(g.x) = (g^{-1}g).x = 1.x = x = g^{-1}.(g.y) = y$. Cela montre que $\varphi(g)$ est injectif. Maintenant soit $x \in E$ donné; alors $(\varphi(g))(g^{-1}(x)) = g(g^{-1}.x) = (g^{-1}g).x = 1.x = x$, donc $\varphi(g)$ est aussi surjectif et en conséquence bijectif.
Montrons que φ est un homomorphisme de groupes. Soient $g, h \in G$ et $x \in E$. Alors $(\varphi(gh))(x) = (gh).x = g.(h.x) = (\varphi(g))((\varphi(h))(x) = (\varphi(g) \circ \varphi(h))(x)$, donc $\varphi(gh) = \varphi(g) \circ \varphi(h)$.
(b) Il suffit de vérifier les deux axiomes : $1.x = (\varphi(1))(x) = \mathrm{id}(x) = x$ et $g.(h.x) = \varphi(g) \circ \varphi(h)(x) = \varphi(gh)(x) = (gh).x$ pour tout $g, h \in G$.
(c) Clair. □

Définition 20.12. *(a) Soit $x \in E$. L'ensemble $G.x = \{g.x \mid g \in G\}$ est appelé* l'orbite de *x (en anglais : orbit, en allemand : Bahn). L'ensemble des orbites est noté $G\backslash E$.*

(b) Soit $x \in E$. L'ensemble $G_x = \{g \in G \mid g.x = x\}$ est appelé le stabilisateur *(ou* groupe d'isotropie*) de x.*

(c) S'il existe $x \in E$ tel que $G.x = E$, on dit que l'opération de G sur E est transitive.

(d) Soit $\pi : G \to S_E$ l'homomorphisme associé à l'opération de G sur E dans le lemme 20.11. S'il est injectif, on dit que l'opération de G sur E est fidèle *(faithful, treu).*

Lemme 20.13. *Le stabilisateur G_x est un sous-groupe de G.*

Démonstration. Soient $g, h \in G_x$. Notons d'abord que l'application de g^{-1} à $g.x = x$ donne $g^{-1}.(g.x) = g^{-1}.x$, donc $g^{-1}.x = (g^{-1}g).x = 1.x = x$. Alors $(g^{-1}h).x = g^{-1}.(h.x) = g^{-1}.x = x$, donc $g^{-1}h \in G_x$, d'où G_x est un sous-groupe de G. □

Exemple 20.14. *(a) Considérons le 5-gone régulier. L'orbite de n'importe quel sommet est l'ensemble de tous les sommets, donc l'opération est transitive. Le stabilisateur de n'importe quel sommet est l'identité et la réflexion à l'axe à travers le centre et le sommet choisi. L'opération est fidèle.*

(b) Considérons l'opération de G sur lui-même par multiplication. Le stabilisateur de $1 \neq g \in G$ est $\{1\}$. Cette action est fidèle et transitive.

En fait, l'homomorphisme $\pi : G \to S_E$ associé à cette opération dans le lemme 20.11 est celui de la proposition 20.2 de Cayley.

(c) Considérons l'opération par conjugaison de G sur lui-même. L'orbite de $h \in G$ est l'ensemble $\{ghg^{-1} \mid g \in G\}$. Si G est abélien, tout $g \in G$ agit comme l'identité. On parle d'une action triviale. Elle n'est certainement pas fidèle (sauf si $G = \{1\}$).

Nous avons la proposition importante suivante.

Proposition 20.15. *Soient E un ensemble et G un groupe. On suppose que G agit sur E.*

(a) La relation binaire $\sim_G$ définie sur E par

$$\forall\,(x, y) \in E^2 : x \sim_G y \iff \exists g \in G : y = g.x$$

est une relation d'équivalence sur E.

Pour tout x dans E, la classe d'équivalence de x pour cette relation est l'orbite de x sous l'action de G.

Comme pour toute relation d'équivalence nous avons la réunion disjointe

$$E = \bigsqcup_{\omega \in G\backslash E} \omega.$$

(b) Pour $x \in E$, l'application $G/G_x \to E$ (de l'ensemble des classes à gauche de G suivant le stabilisateur G_x dans E) donnée par $gG_x \mapsto g.x$ est bien définie et bijective. En particulier, on a $\#G.x = (G : G_x)$ (le cardinal de l'orbite est l'indice du stabilisateur).

(c) Dans toute orbite $\omega \in G\backslash E$ on choisit un représentant x_ω. Alors, on a l'égalité :

$$\#E = \sum_{\omega\in G\backslash E} G.x_\omega = \sum_{\omega\in G\backslash E} (G : G_{x_\omega}) = \#G \cdot \sum_{\omega\in G\backslash E} \frac{1}{\#G_{x_\omega}}$$

où pour la dernière égalité nous supposons G fini. Cette égalité s'appelle formule des classes (Bahnenbilanzgleichung).

Démonstration. (a) Vérification simple et propriétés des relations d'équivalence.
(b)

Bien défini. Montrons que l'application ne dépend pas du choix de représentants : $gG_x = hG_x$, donc $g = h \cdot r$ avec $r \in G_x$. Donc $g.x = (hr).x = h.(r.x) = h.x$ car $r.x = x$.

Injectif. Soient $g.x = h.x$ avec $g, h \in G$. Alors nous avons $h^{-1}.(g.x) = h^{-1}(h.x)$, donc $(h^{-1}g).x = (h^{-1}h).x = 1.x = x$, d'où $h^{-1}g \in G_x$, donc $gG_x = hG_x$.

Surjectif. Soit $g \in G$. Alors gG_x est envoyé sur $g.x$.

(c) suit de (a) et (b). □

Proposition 20.16 (Burnside)**.** *Soient E un ensemble fini et G un groupe fini. Alors*

$$\#(G\backslash E) = \frac{1}{\#G} \sum_{g\in G} \#\mathrm{Fix}_g,$$

où $\mathrm{Fix}_g = \{x \in E \mid g.x = x\}$.

Démonstration. Nous avons

$$\#(G\backslash E) = \sum_{\omega\in G\backslash E} 1 = \sum_{\omega\in G\backslash E} \sum_{x\in\omega} \frac{1}{\#\omega} = \sum_{\omega\in G\backslash E} \sum_{x\in\omega} \frac{1}{\#Gx}$$
$$= \sum_{x\in E} \frac{1}{\#Gx} = \sum_{x\in E} \frac{\#G_x}{\#G} = \frac{1}{\#G} \sum_{x\in E} \#G_x.$$

Pour $g \in G$ et $x \in E$ nous posons

$$\delta_{g,x} = \begin{cases} 1 & \text{si } g.x = x, \\ 0 & \text{sinon.} \end{cases}$$

Nous obtenons

$$\sum_{x\in E} \#G_x = \sum_{x\in E} \sum_{g\in G} \delta_{g,x} = \sum_{g\in G} \sum_{x\in E} \delta_{g,x} = \sum_{g\in G} \#\mathrm{Fix}_g.$$

La formule de Burnside est montrée. □

Exemple 20.17. *Nous déterminons le nombre de colliers différents à 5 perles mobiles sur un fil dont les couleurs sont rouge, blanc ou bleu. C'est une application de la formule de Burnside.*

On peut s'imaginer les 5 *perles comme les sommets (coloriés en rouge, blanc ou bleu) d'un* 5*-gone régulier. Soit* E *l'ensemble de tous les* 5*-gones dont les sommets sont rouge, blanc ou bleu. Alors* $\#E = 3^5 = 243$*.*
Comme nous l'avons vu, toute symétrie du 5*-gone donne le même collier, et si deux* 5*-gones coloriés donnent le même collier, alors il s'agit d'une symétrie. En d'autres mots, le groupe* $G = D_5$ *agit sur* E*. Le nombre de colliers différents est le nombre d'orbites pour cette action. Nous pouvons donc utiliser la formule de Burnside.*
Si $g = \mathrm{id}$*, alors* $\#\mathrm{Fix}_{\mathrm{id}} = 3^5$*. Si* g *est une des 4 rotations non-triviales, alors seuls les colliers d'une seule couleur sont fixés ; il y en a trois (un par couleur). Si* g *est une des* 5 *réflexions, alors le sommet fixé peut avoir n'importe quelle couleur ; les quatres autres sommets forment deux couples qui sont échangés ; chaque couple peut avoir n'importe quelle couleur ; donc* 3^3 *éléments sont fixés.*
En conséquence, il existe

$$\#(G\backslash E) = \frac{1}{\#D_5}(3^5 + 4 \cdot 3 + 5 \cdot 3^3) = \frac{243 + 12 + 135}{10} = 39$$

colliers différents.

Exemple 20.18. *Considérons une variante de l'opération de* G *sur lui-même par multiplication, donc de l'homomorphisme de Cayley de la proposition 20.2. Soit* G *un groupe et* $H \subseteq G$ *un sous-groupe. Posons* $E = G/H$*, l'ensemble des classes à gauche suivant* H*.* G *agit sur* G/H *par multiplication :* $g_1.(g_2H) := (g_1g_2).H$ *pour tout* $g_1, g_2 \in G$*. En d'autres mots, nous avons l'homomorphisme*

$$\varphi : G \to S_{G/H}, \quad g_1 \mapsto (g_2H \mapsto (g_1g_2)H)$$

avec $S_{G/H}$ *le groupe symétrique.*
Comme application de cette opération, nous montrons l'assertion suivante (qui généralise le fait (exercice) que tout sous-groupe d'indice 2 *d'un groupe fini est normal).*

> Soit $G \neq \{1\}$ un groupe fini et soit p le nombre premier le plus petit tel que $p \mid \#G$.
> Alors tout sous-groupe H de G d'indice p est normal.

Calculons le noyau de φ*. On cherche donc les* $g_1 \in G$ *tels que* $g_1g_2H = g_2H$ *pour tout* $g_2H \in G/H$ *ou, de façon équivalente, les* $g_1 \in G$ *qui appartiennent à* $g_2Hg_2^{-1}$ *pour tout* $g_2 \in G$*. Le noyau de* φ *est donc* $\bigcap_{g\in G} gHg^{-1}$*.*
Soit maintenant H *d'indice* p *où* p *est le plus petit premier divisant* $\#G$*. Donc le cardinal de* $S_{G/H}$ *est* $p!$*. Par le théorème d'isomorphisme et le théorème de Lagrange, le cardinal de* $G/\ker(\varphi)$ *divise* $p!$*. Il est clair que* $\ker(\varphi) \subseteq H$*. Par la généralisation du théorème de Lagrange (exercice) nous avons*

$$(G : \ker(\varphi)) = (G : H) \cdot (H : \ker(\varphi)) = p \cdot (H : \ker(\varphi)).$$

On conclut que $(H : \ker(\varphi))$ *divise* $(p-1)!$ *et* $(G : \ker(\varphi)) = \frac{\#G}{\#\ker(\varphi)}$*, donc* $\#G$*. Comme* $\#G$ *n'est pas divisible par un premier strictement plus petit que* p*, on obtient* $(H : \ker(\varphi)) = 1$*, donc* $H = \ker(\varphi)$*. En tant que noyau d'un homomorphisme,* H *est un sous-groupe normal.*

21 Supplément : Les théorèmes de Sylow

Avant de démontrer les théorèmes de Sylow, nous étudions de plus près l'opération d'un groupe G sur lui-même par conjugaison (voir l'exemple 20.14)

$$G \times G \to G, \quad (g,h) \mapsto ghg^{-1}.$$

Définition 21.1. *Soit G un groupe. Le stabilisateur de $h \in G$ pour l'opération de G sur lui-même par conjugaison*

$$Z_h := Z_h(G) := \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\}$$

est appelé le centralisateur de h dans G. *C'est un sous-groupe de G car les stabilisateurs le sont toujours.*
Soit $H \subseteq G$ un sous-ensemble. Le centralisateur de H dans G *est défini comme*

$$Z_H(G) := \{g \in G \mid \forall\, h \in H : gh = hg\} = \bigcap_{h \in H} Z_h(G).$$

C'est un sous-groupe car une intersection de sous-groupes est toujours un sous-groupe.

Exemple 21.2. *(a) $Z_G(G)$ est le centre $\mathcal{Z}(G)$ de G, c'est-à-dire, l'ensemble $\{g \in G \mid \forall\, h \in G : gh = hg\}$.*

(b) Pour $g \in G$, on a l'équivalence $g \in \mathcal{Z}(G) \Leftrightarrow Z_g(G) = G$.

En particulier, l'orbite de $g \in \mathcal{Z}(G)$ pour la conjugaison est $\{g\}$.

(c) $Z_{(1\,2\,3)}(S_3) = \langle (1\,2\,3) \rangle$.

Corollaire 21.3. *Soit G un groupe fini. Pour toute orbite de cardinal ≥ 2 (pour l'action de G sur lui-même par conjugaison), on choisit un représentant x_i. Soit n le nombre de telles orbites. On a*

$$G = \bigsqcup_{g \in \mathcal{Z}(G)} \{g\} \sqcup \bigsqcup_{i=1}^{n} \{gx_ig^{-1} \mid g \in G\}$$

et donc

$$\#G = \#\mathcal{Z}(G) + \sum_{i=1}^{n} (G : Z_{x_i}(G))$$

avec $Z_{x_i}(G) \neq G$ pour tout $i = 1, \ldots, n$.

Démonstration. C'est précisement la formule des orbites de la proposition 20.15 (c) appliquée à l'action de G sur lui-même par conjugaison. □

Nous sommes maintenant prêts pour le premier théorème de Sylow. D'abord il s'agit de mettre en place la terminologie nécessaire.

Définition 21.4. *Soit p un nombre premier. On appelle p-*groupe *tout groupe fini d'ordre p^n pour un $n \in \mathbb{N}$.*

Exemple 21.5. *(a) Le groupe $G = \{1\}$ d'ordre $p^0 = 1$ est un p-groupe pour tout nombre premier p.*

(b) $\mathbb{Z}/p\mathbb{Z}$ est un p-groupe de cardinal $p = p^1$.

(c) $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ est un p-groupe de cardinal p^2.

(d) L'ensemble des matrices

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

est un p-groupe de cardinal p^3 pour la multiplication de matrices. Ce groupe n'est pas abélien.

Définition 21.6. *Soit G un groupe fini de cardinal $n = p^r m$ où p est un nombre premier tel que $p \nmid m$. On appelle p-*groupe de Sylow *(ou p-*Sylow*) tous sous-groupe $H \leq G$ de cardinal $\#H = p^r$.*
En d'autres mots, un p-groupe de Sylow est un sous-groupe qui est un p-groupe de cardinal égal à la plus grande puissance de p qui divise le cardinal de G.

Exemple 21.7. *(a) Si $p \nmid \#G$, alors $\{1\}$ est un p-groupe de Sylow de G.*

(b) Prenons $G = S_3$ de cardinal 6. Il existe trois 2-groupes de Sylow : $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$. Il n'existe qu'un seul 3-groupe de Sylow : $\langle(1\ 2\ 3)\rangle$.

(c) Prenons $G = A_4$ de cardinal $12 = 2^2 \cdot 3$. Il existe un 2-groupe de Sylow :

$$\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Il existe plusieurs 3-groupes de Sylow : $\langle(1\ 2\ 3)\rangle$, $\langle(1\ 2\ 4)\rangle$, etc.

Lemme 21.8. *Soit G un groupe fini de cardinal $\#G = m$ et p un nombre premier qui divise m. Alors il existe $g \in G$ d'ordre p.*

Démonstration. Supposons le contraire : il n'existe aucun élément de g d'ordre p. On numérote les éléments de G : $1 = g_0, g_1, g_2, \ldots, g_{m-1}$. Prenons le produit cartésien $C := \prod_{i=1}^{m-1} \langle g_i \rangle$. C'est un ensemble de cardinal égal à

$$\prod_{i=1}^{m-1} \#\langle g_i \rangle = \prod_{i=1}^{m-1} \operatorname{ord}(g_i).$$

Par notre hypothèse le cardinal de C n'est pas divisible par p. Notons que C est un groupe pour la loi interne « composante par composante ». L'application

$$\varphi : C \to G, \quad (g_1^{e_1}, g_2^{e_2}, \ldots, g_{m-1}^{e_{m-1}}) \mapsto \prod_{i=1}^{m-1} g_i^{e_i}$$

est un homomorphisme de groupes qui est surjectif. Donc le cardinal de G est égal au cardinal $\#C/\#\ker(\varphi)$, donc c'est un diviseur de $\#C$. En conséquence, p ne peut pas diviser $\#G$ non-plus. Contradiction. □

Dans la démonstration à venir nous avons besoin d'un petit lemme que nous aurions pu déjà montrer plus tôt.

Lemme 21.9. *Soit $\pi : G \to H$ un homomorphisme surjectif de groupes. Soit $V \subseteq H$ un sous-groupe et $U = \pi^{-1}(V)$ le sous-groupe de G obtenu comme image réciproque.*
Alors nous avons l'égalité d'indices $(G : U) = (H : V)$.

Démonstration. Considérons l'application

$$\varphi : G/U \to H/V, \quad gU \mapsto \pi(g)V.$$

Elle est bien définie car si $g_1U = g_2U$, alors $g_2^{-1}g_1 \in U$, donc $\pi(g_2^{-1}g_1) \in V$ d'où $\pi(g_1)V = \pi(g_2)V$. Elle est surjective : soit $hV \in H/V$ une classe donnée ; la surjectivité de π nous permet de choisir $g \in G$ tel que $\pi(g) = h$; donc $\varphi(gU) = \pi(g)V = hV$. Finalement, φ est aussi injectif. Supposons que nous avons deux classes $g_1U, g_2U \in G/U$ telles que $\varphi(g_1U) = \varphi(g_2U)$, donc $\pi(g_1)V = \pi(g_2)V$ d'où $\pi(g_2^{-1}g_1) \in V$, alors $g_2^{-1}g_1 \in \pi^{-1}(V) = U$ ce qui implique $g_1U = g_2U$.
Comme φ est bijectif, on a $(G : U) = (H : V)$. □

Théorème 21.10 (1er théorème de Sylow)**.** *Soient G un groupe fini et p un nombre premier. Alors G possède un p-groupe de Sylow.*

Démonstration. Récurrence sur le cardinal m de G.
L'initialisation $\#G = m = 1$ est triviale.
Supposons le théorème démontré pour tout groupe de cardinal strictement inférieur à m. Soit G un groupe de cardinal m. Si $p \nmid m$, le groupe $\{1\}$ est un p-groupe de Sylow, comme nous l'avons vu. Soit donc $m = p^e r$ avec $p \nmid r$ et $e \geq 1$. Nous utilisons la formule des orbites du corollaire 21.3 :

$$\#G = \#\mathcal{Z}(G) + \sum_{i=1}^{n} (G : Z_{x_i}(G))$$

avec $Z_{x_i}(G) \neq G$ pour tout $i = 1, \ldots, n$.

1er cas : $p \nmid \#\mathcal{Z}(G)$. De la formule des orbites il suit qu'il existe $i \in \{1, 2, \ldots, n\}$ tel que

$$p \nmid (G : Z_{x_i}(G)) = \frac{\#G}{\#Z_{x_i}(G)} = \frac{p^e r}{\#Z_{x_i}(G)}.$$

Donc $p^e \mid \#Z_{x_i}(G)$. Comme $Z_{x_i}(G) \neq G$, on a $\#Z_{x_i}(G) < m$ ce qui nous permet d'utiliser l'hypothèse de récurrence : $Z_{x_i}(G)$ contient un p-groupe P de cardinal p^e. Ce groupe est un p-groupe de Sylow pour G.

2ème cas : $p \mid \#\mathcal{Z}(G)$. Comme $\mathcal{Z}(G)$ est abélien, le lemme 21.8 implique qu'il existe $g \in \mathcal{Z}(G)$ d'ordre p. Soit $N = \langle g \rangle$ le sous-groupe cyclique engendré par g. Comme g commute avec tous les éléments de G, le sous-groupe N est distingué. Nous pouvons donc prendre le quotient $\overline{G} := G/N$. C'est un groupe de cardinal $m/p = p^{e-1}r$, donc l'hypothèse de récurrence s'applique. Nous obtenons un sous-groupe $\overline{P} \subseteq \overline{G}$ de cardinal p^{e-1}. Pour produire un p-groupe de Sylow dans G, nous considérons la projection $\pi : G \twoheadrightarrow \overline{G} = G/N$ qui envoie g sur sa classe gN. Posons $P := \pi^{-1}(\overline{P})$. Nous savons (c'est un fait général qui n'utilise rien de notre situation particulière ici) que P est un sous-groupe de G et par le lemme 21.9 on obtient $\frac{\#G}{\#P} = (G : P) = (\overline{G} : \overline{P}) = r$ d'où $\#P = p^e$ est un p-groupe de Sylow.

La démonstration est achevée. □

Lemme 21.11. *Soit P un p-groupe de Sylow de G. Alors pour tout $g \in G$, le groupe gPg^{-1} est aussi un p-groupe de Sylow.*

Démonstration. C'est clair car l'application $P \to gPg^{-1}$ qui envoie $h \in P$ sur ghg^{-1} est une bijection d'inverse $gPg^{-1} \to P$ telle que $h' \in gPg^{-1}$ est envoyé sur $g^{-1}h'g$. Il est clair que ces deux applications sont surjectives ; donc $\#P \geq gPg^{-1}$ et $\#P \leq gPg^{-1}$ d'où l'égalité recherchée. □

Considérons maintenant une autre opération. Soit G toujours un groupe. Soit

$$E = \{H \mid H \subseteq G \text{ sous-groupe}\},$$

l'ensemble de tous les sous-groupes de G. Le groupe G agit sur E par conjugaison :

$$G \times E \to E, \quad (g, H) \mapsto gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Définition 21.12. *Le* normalisateur de H dans G *est défini comme le stabilisateur de H pour l'opération décrite ci-dessus :*

$$N_H(G) := \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\}.$$

Le normalisateur est un sous-groupe car tout stabilisateur pour toute opération est un sous-groupe. En plus, on a toujours $H \trianglelefteq N_H(G)$.

Exemple 21.13. *(a)* $N_{\langle(1\,2\,3)\rangle}(S_3) = S_3$.

(b) Plus généralement, si $H \trianglelefteq G$ est normal, alors $N_H(G) = G$.

Soit $\mathcal{S}_p$ le sous-ensemble (non-vide à cause du théorème 21.10) de E de tous les p-groupes de Sylow. Le lemme 21.11 implique que l'opération de G sur E laisse $\mathcal{S}_p$ invariant.

Proposition 21.14. *Soit G un groupe fini et P un p-groupe de Sylow. Soit $H \subseteq G$ un sous-groupe qui est un p-groupe.*

(a) Si $hPh^{-1} = P$ pour tout $h \in H$, alors $H \subseteq P$.

(b) Il existe $g \in G$ tel que $S = gPg^{-1}$ est un p-groupe de Sylow avec $H \subseteq S$. En particulier, tout p-groupe est contenu dans un p-groupe de Sylow.

Démonstration. (a) L'hypothèse implique $H \subseteq N_P(G)$ et on a, comme toujours, $P \trianglelefteq N_P(G)$. En conséquence (voir le lemme 1.15 (c)), HP est un sous-groupe de $N_P(G)$. Le 2ème théorème d'isomorphisme 1.16 donne

$$HP/P \cong H/H \cap P.$$

Donc HP est un p-groupe (car $\frac{\#HP}{\#P}$ est une puissance de p car c'est un diviseur de $\#H$) qui contient P. Donc $HP = P$ car S est un p-groupe de Sylow. On en conclut que $H \subseteq P$.
(b) Comme nous l'avons vu, le stabilisateur de l'opération de G par conjugaison sur P est le normalisateur $N_P(G)$ de P dans G. Soit $G.P = \{gPg^{-1} \mid g \in G\}$ l'orbite. Par la proposition 20.15 (b) nous avons $\#G.P = \#G/\#N_P(G)$. Comme $P \subseteq N_P(G)$, on a $p^e \mid N_P(G)$, donc $p \nmid \#G.P$.

Soit H maintenant un sous-groupe de G qui est un p-groupe. Nous avons que H agit sur l'orbite $G.P$ par conjugaison. Considérons la réunion disjointe des orbites pour cette action :

$$G.P = \bigsqcup_{i=1}^{s} \{hg_iPg_i^{-1}h^{-1} \mid h \in H\}.$$

Encore la proposition 20.15 (b) nous dit que le cardinal de toute orbite de H est un diviseur de $\#H$, donc c'est une puissance de p. Comme le cardinal de $G.P$ n'est pas divisible par p, il doit y avoir au moins une classe $\{hg_kPg_k^{-1}h^{-1} \mid h \in H\}$ de cardinal $p^0 = 1$.
On pose $S = g_kPg_k^{-1}$. C'est un p-groupe de Sylow et par ce qui précède (cardinal de l'orbite pour H est 1), pour tout $h \in H$ on a $hSh^{-1} = S$. Donc (a) donne le résultat. □

Théorème 21.15 (2ème théorème de Sylow)**.** *Soit G un groupe fini. Si $P_1, P_2 \subseteq G$ sont des p-groupes de Sylow, alors il existe $g \in G$ tel que $gP_1g^{-1} = P_2$.*
En d'autres mots, l'action par conjugaison de G sur l'ensemble $\mathcal{S}_p$ des p-groupes de Sylow est transitive.

Démonstration. Il suffit de prendre $H = P_2$ et $P = P_1$ dans la proposition 21.14. □

Théorème 21.16 (3ème théorème de Sylow)**.** *Soient G un groupe fini et p un nombre premier. Soit s_p le nombre des p-groupes de Sylow de G. Alors, $s_p \mid \#G$ et $s_p \equiv 1 \mod p$.*

Démonstration. Comme l'opération de G sur $\mathcal{S}_p$ est transitive par le deuxième théorème de Sylow 21.15, $\mathcal{S}_p$ est une orbite et donc son cardinal s_p est un diviseur de $\#G$ par la proposition 20.15 (b). Soit P un p-groupe de Sylow. Au lieu de l'action de G sur $\mathcal{S}_p$, on considère maintenant l'action de P et ses orbites. Une des orbites, c'est $\{P\}$. Pour $g \in G$, soit $\{hgPg^{-1}h^{-1} \mid h \in P\}$ une autre orbite. Par la proposition 20.15 (b) et le fait que P est un p-groupe, soit le cardinal de cette orbite est 1, soit divisible par p. Si on est dans le premier cas, on a $hgPg^{-1}h^{-1} = gPg^{-1}$ pour tout $h \in P$. Donc la proposition 21.14 (a) implique $P \subseteq gPg^{-1}$, alors $P = gPg^{-1}$ à cause du fait que les deux ensembles sont du même cardinal. Cela veut dire que $\{P\}$ est la seule orbite pour l'action de P de cardinal 1. Toutes les autres orbites sont de cardinal divisible par p.
Comme $\mathcal{S}_p$ est la réunion disjointe des orbites pour l'action de P, on obtient $s_p \equiv 1 \mod p$. □

Corollaire 21.17. *Soit G un groupe fini et p un nombre premier.*

(a) Si $p \mid \#G$, alors il existe $g \in G$ d'ordre p.

(b) G est un p-groupe si et seulement si l'ordre de tout élément de G est une puissance de p.

Démonstration. (a) Soit P un p-groupe de Sylow de G et soit $g \in P$ un élément différent de 1. Alors l'ordre de g est une puissance de p, disons p^r. En conséquence, $h := g^{p^{r-1}}$ est d'ordre p.
(b) La seule chose non-triviale est que G est un p-groupe. Si cela n'était pas le cas, alors par (a) on aurait un élément d'ordre p' avec p' un premier différent de p. □

Corollaire 21.18. *Soit G un groupe fini et p un nombre premier. Si G possède exactement un p-groupe de Sylow P, alors P est normal.*

Démonstration. On sait que pour tout $g \in G$, le groupe gPg^{-1} est aussi un p-groupe de Sylow. Comme il n'y en a qu'un seul, on a $gPg^{-1} = P$ pour tout $g \in G$ d'où P est normal. □

Corollaire 21.19. *Soient $p < q$ deux nombres premiers tels que $p \nmid (q-1)$. Alors tout groupe G de cardinal pq est cyclique.*

Démonstration. Par le troisième théorème de Sylow 21.16, nous avons $s_p \equiv 1 \mod p$, $s_q \equiv 1 \mod q$ et $s_p, s_q \mid pq$. Cela laisse les possibilités $s_p \in \{1, q\}$ et $s_q \in \{1, p\}$. Maintenant l'hypothèse $q \not\equiv 1 \mod p$ intervient pour exclure $s_p = q$, donc $s_p = 1$. Le fait $p < q$ implique aussi $p \not\equiv 1 \mod q$, d'où $s_q = 1$. Il existe donc un unique p-groupe de Sylow P et un unique q-groupe de Sylow Q de cardinal p, q, respectivement. Par le lemme 1.15, nous avons que PQ est un sous-groupe de G, donc égal à G car il est du même cardinal.
Soient maintenant $x \in P$ et $y \in Q$. L'élément $xyx^{-1}y^{-1}$ est dans P (car $yx^{-1}y^{-1} \in P$ à cause de la normalité de P) et dans Q (car $xyx^{-1} \in Q$ à cause de la normalité de Q). Comme $P \cap Q = \{1\}$ (car l'ordre de tout élément dans l'intersection doit être un diviseur commun de p et q, donc est égal à 1), on a $xyx^{-1}y^{-1} = 1$, donc $xy = yx$. Le groupe G est donc abélien.
Soit $g \in P \setminus \{1\}$ et $h \in Q \setminus \{1\}$. L'ordre de gh est $\mathrm{ppcm}(p, q) = pq$. Donc G est cyclique. □

Exemple 21.20. *Si G est un groupe d'ordre 35, alors G est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/35\mathbb{Z}$. Effectivement, $5 \nmid (7-1)$.*

Définition 21.21. *Un groupe G est dit* simple *si ses seuls sous-groupes normaux sont $\{1\}$ et G.*

Exemple 21.22. *Aucun groupe de cardinal $30 = 2 \cdot 3 \cdot 5$ n'est simple.*
Par le troisième théorème de Sylow 21.16, nous avons $s_p \equiv 1 \mod p$ et $s_p \mid 2 \cdot 3 \cdot 5$ pour $p = 2, 3, 5$. Cela laisse les possibilités

$$s_2 \in \{1, 3, 5, 15\}, \quad s_3 \in \{1, 10\}, \quad s_5 \in \{1, 6\}.$$

Supposons $s_3 > 1$ et $s_5 > 1$, donc $s_3 = 10$ et $s_5 = 6$.
Soient $P_1, \ldots, P_6$ les six 5-groupes de Sylow. Comme $P_i \cap P_j = \{1\}$ pour $i \neq j$, les 5 groupes de Sylow contiennent $6 \cdot 4 = 24$ éléments d'ordre 5.
Soient $Q_1, \ldots, Q_{10}$ les dix 3-groupes de Sylow. Avec le même argument, ils contiennent $10 \cdot 2 = 20$ éléments d'ordre 3.
En tout, nous avons trouvé 44 éléments d'ordre 3 et 5, ce qui est évidemment une contradiction avec le cardinal 30.
En conséquence, soit $s_3 = 1$ (dans ce cas le seul 3-Sylow est normal), soit $s_5 = 1$ (dans ce cas le seul 5-Sylow est normal).