Cours d'algèbre générale
M2 Préparation à l'agrégation

14 octobre 2026

Table des matières

1 Groupes et actions de groupes **3**
1.1 Action de groupe 3
1.2 Conjugaison 6
1.3 Les p-groupes 10
1.4 Groupes finis usuels 13

2 Anneaux via des exemples **17**
2.1 Exemples d'anneaux d'entiers 17
2.2 Exemples d'anneaux de polynômes 19

3 Extensions de corps et corps finis **24**
3.1 Extensions de corps : définitions 24
3.2 Clôture algébrique 27
3.3 Corps finis 29

4 Polynômes **33**
4.1 Propriété universelle des algèbres de polynômes 33
4.2 Polynômes irréductibles 33
4.3 Polynômes à plusieurs variables 37
4.4 Polynômes cyclotomiques 39

5 Formes quadratiques **42**
5.1 Définitions 42
5.2 Classes de congruence 43
5.3 Classification des formes quadratiques 45

1 Groupes et actions de groupes

Dans cette section on rappelle plusieurs définitions et résultats fondamentaux concernant l'action d'un groupe sur un ensemble. On suppose connues les notions de base (groupe, groupe abélien, sous-groupe, produit direct de groupes, morphisme de groupes, noyau et image d'un morphisme de groupes, ordre d'un élément, etc...).

1.1 Action de groupe

(•) Définition.

Soit G un groupe (de neutre noté e) et X un ensemble. On note $\mathrm{Bij}(X)$ l'ensemble des bijections de X. Une action (à gauche) de G sur X est la donnée d'un morphisme de groupes

$$\varphi : G \to \mathrm{Bij}(X).$$

On note alors $g \cdot x = \varphi(g)(x)$.

De manière équivalente, on peut définir une action (à gauche) de G sur X comme la donnée d'une application $\mu : G \times X \to X$ telle que pour tout g, h dans G et x dans X, on a

$$\mu(gh, x) = \mu(g, \mu(h, x)) \text{ et } \mu(e, x) = x.$$

On notera

$$g \cdot x := \mu(g, x).$$

Définition 1.1. L'action est dite fidèle si $\mathrm{Ker}(\varphi) = 1$.

On rappellera plus loin les notions de sous-groupes distingués et groupe quotient. En particulier, on obtient que le groupe quotient $G/\mathrm{Ker}(\varphi)$ agit toujours fidèlement sur X.

(•) Stabilisateur, liberté et orbites.

Le stabilisateur d'un point x de X est défini par

$$G_x := \mathrm{Stab}_G(x) := \{g \in G,\ g \cdot x = x\}.$$

C'est un sous-groupe de G. Si Y est un partie de X on définit les deux notions suivantes (à ne pas confondre) :

$$G_{\{Y\}} := \mathrm{Stab}_G(\{Y\}) := \{g \in G,\ g \cdot Y = Y\} \text{ où } g \cdot Y := \{g \cdot y,\ y \in Y\}.$$

$$G_Y := \mathrm{Stab}_G(Y) := \{g \in G,\ g \cdot y = y \quad \forall y \in Y\} = \bigcap_{y \in Y} \mathrm{Stab}_G(y).$$

On définit les points fixes :

— d'un élément g de G : $X^g := \{x \in X,\ g \cdot x = x\} = \{x \in X,\ g \in \mathrm{Stab}_G(x)\}$,

— d'un sous-groupe H de G : $X^H = \bigcap_{h \in H} X^h$.

Proposition 1.2. *Pour tout x dans X et g dans G, on a*

$$\mathrm{Stab}_G(g \cdot x) = g\mathrm{Stab}_G(x)g^{-1}$$

En particulier, si l'action de G sur X est transitive (voir ci-dessous), alors les stabilisateurs d'un point sont des sous-groupes conjugués dans G.

Démonstration. Exercice. □

Définition 1.3. Une action est dite libre si tous les stabilisateurs sont triviaux, ou de manière équivalente si tous les ensembles de points fixes X^g pour $g \neq e$ sont vides.

Proposition 1.4. *Une action libre est fidèle.*

Démonstration. Évident en écrivant les définitions. □

Si x est un élément de X, l'orbite de x pour l'action de G est la partie de X définie par

$$\mathcal{O}(x) := G \cdot x = \{g \cdot x,\ g \in G\}.$$

La relation "être dans une même orbite" est une relation d'équivalence, donc "X" se partitionne en orbites. Indexons l'ensemble des orbites par I. Pour chaque orbite d'index i, on choisit un élément x_i dans l'orbite. On obtient ainsi une famille de représentants $(x_i)_{i \in I}$.

Proposition 1.5. *On suppose que G et X sont finis. Alors,*

(1) Équation aux classes : pour tout x de X, on a

$$|G \cdot x| = [G : \mathrm{Stab}_G(x)].$$

(2) Formule des classes : si $(x_i)_{i \in I}$ est une famille de représentants, on a

$$|X| = \sum_{i \in I} [G : \mathrm{Stab}_G(x_i)]$$

Démonstration. Le deuxième point découle immédiatement du premier en utilisant que $(x_i)_{i \in I}$ est une famille de représentants pour l'action de G sur X. Pour le premier point, on utilise la bijection de $G/\mathrm{Stab}_G(x)$ dans $G \cdot x$ qui envoie la classe $g\mathrm{Stab}_G(x)$ sur $g \cdot x$. □

Définition 1.6. (1) L'action de G sur X est dite transitive s'il n'y a qu'une seule orbite $G \cdot x = X$ pour tout x de X, ou de manière équivalente, si pour tous x et y dans X, il existe g dans G tel que $g \cdot x = y$.

(2) L'action est dite simplement transitive si elle est libre et transitive.

(3) Pour n dans N, l'action de G sur X est dite n-transitive si l'action de G sur l'ensemble des parties à n éléments $\mathcal{P}_n(X)$ est transitive. Une action est dite exactement n-transitive si elle est n-transitive mais pas $(n+1)$-transitive.

Exemple 1.7. (1) Pour K un corps, l'action de $\mathrm{GL}(K^n)$ sur l'ensemble des bases de K^n est simplement transitive.

(2) L'action de $\mathfrak{S}_n$ sur $[|1, n|]$ est m-transitive pour tout $m \leq n$.

(3) Il est également possible de montrer que l'action de $\mathrm{PGL}_2(K) = \mathrm{GL}_2(K)/K^*$ sur $\mathbf{P}^1(K)$ donnée par

$$g \cdot z = \frac{az+b}{cz+d} \quad \text{pour} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } z \in \mathbf{P}^1(K),$$

est exactement 3-transitive.

(•) Formule de Burnside.

On verra en TD la démonstration et des applications de la formule de Burnside :

Proposition 1.8. *Soit G un groupe fini qui agit sur un ensemble X fini. Alors*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Exemple 1.9. La formule de Burnside permet par exemple de montrer que tout sous-groupe de $\mathfrak{S}_n$ agissant transitivement sur $[|1, n|]$ contient une permutation sans points fixes.

(•) Action par translation de G sur lui-même.

Le groupe G agit sur lui-même par multiplication à gauche, i.e. $g \cdot h = gh$ (respectivement par multiplication par l'inverse à droite : $g \cdot h = hg^{-1}$). Cette action est simplement transitive. Si H est un sous-groupe de G alors par restriction on obtient une action de H sur G. On appelle classe à gauche (respectivement classe à droite) les orbites Hg (respectivement gH) de cette action. L'indice d'un sous-groupe H de G noté $[G : H]$ est le nombre d'orbites pour cette action.

Proposition 1.10 (Théorème de Lagrange)**.** *Soit G un groupe fini et H un sous-groupe de G. L'ordre de H divise toujours l'ordre de G. En particulier, l'ordre d'un élément divise l'ordre du groupe.*

Démonstration. On fabrique une partition de G à partir des ensembles gH pour g dans G. Si n est le nombre d'ensembles nécessaires pour réaliser cette partition, on a

$$n|H| = |G|$$

et donc l'ordre de H divise celui de G.

□

Proposition 1.11 (Théorème de Cayley)**.** *Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Démonstration. L'ensemble $\mathrm{Bij}(G)$ des bijections de G sur lui-même est un groupe isomorphe à $\mathfrak{S}_n$. Considérons le morphisme φ de G dans $\mathrm{Bij}(G)$ donnée par $g \mapsto (h \mapsto gh)$. Il est injectif : son image définit donc bien un sous-groupe de $\mathfrak{S}_n$. □

1.2 Conjugaison

(•) **Action par conjugaison.** Soit G un groupe. Alors G agit sur lui-même par conjugaison, i.e. la flèche

$$\varphi : \begin{cases} G & \to \mathrm{Bij}(G) \\ g & \mapsto \mathrm{Int}(g) := (h \mapsto ghg^{-1}). \end{cases}$$

est un morphisme de groupes. Une orbite pour cette action est appelée classe de conjugaison.

Exemple 1.12. (1) Les classes de conjugaison de $\mathfrak{S}_n$ sont décrites par les tailles des cycles dans une décomposition en produit de cycles à supports disjoints.

(2) Les classes de conjugaison dans $\mathrm{GL}_2(\mathbf{C})$ sont données par

$$\{M \in \mathcal{M}_2(\mathbf{C}) \text{ telle que } \mu_M = (X-\lambda_1)(X-\lambda_2)\},$$
$$\{M \in \mathcal{M}_2(\mathbf{C}) \text{ telle que } \mu_M = (X-\lambda)^2\},$$
$$\{\lambda \cdot \mathrm{Id}\}$$

pour $\lambda, \lambda_1, \lambda_2$ dans $K^\times$ tels que $\lambda_1 \neq \lambda_2$. Ici μ_M désigne le polynôme minimal de la matrice M.

Les éléments de $\mathrm{Im}(\varphi)$ sont des automorphismes du groupe G et on les appelle automorphismes intérieurs. On note

$$\mathrm{Int}(G) = \mathrm{Im}(\varphi) \text{ et } \mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G).$$

Remarquons que le sous-groupe $\mathrm{Int}(G)$ est distingué (voir ci-dessous) dans $\mathrm{Aut}(G)$ donc $\mathrm{Out}(G)$ est un groupe.

Le noyau de φ est noté $\mathcal{Z}(G)$ et est appelé le centre de G. C'est l'ensemble des éléments de G qui commutent avec tous les éléments de G, i.e.

$$\mathcal{Z}(G) = \{z \in G \mid zg = gz \text{ pour tout } g \in G\}.$$

Par construction, on a un isomorphisme

$$\mathrm{Int}(G) \simeq G/\mathcal{Z}(G).$$

Lemme 1.13. *(1) L'action par conjugaison de G sur lui-même est fidèle si et seulement si $\mathcal{Z}(G) = 1$. En particulier, si G est abélien, l'action par conjugaison n'est jamais fidèle.*

(2) L'action par conjugaison de G sur lui-même est libre si et seulement si $G = 1$.

Démonstration. Exercice. □

Définition 1.14. Si X est une partie de G, on définit :

(1) le centralisateur de X dans G, noté $\mathcal{Z}_G(X)$: c'est le stabilisateur point par point $\mathrm{Stab}_G(X)$ de X pour l'action par conjugaison de G sur lui-même, i.e.

$$\mathcal{Z}_G(X) = \{g \in G \mid \forall x \in X, gxg^{-1} = x\},$$

(2) le normalisateur de X dans G, noté $\mathcal{N}_G(X)$: c'est le stabilisateur $\mathrm{Stab}_G(\{X\})$ de la partie X, i.e.

$$\mathcal{N}_G(X) = \{g \in G \mid gXg^{-1} = X\}.$$

Définition 1.15. On dit qu'un sous-groupe H est normal si $\mathcal{N}_G(H) = G$. On dit qu'il est central si $\mathcal{Z}_G(H) = G$.

En particulier, on a :

Proposition 1.16. *Si H est un sous-groupe de G, le normalisateur de H est le plus grand sous-groupe de G dans lequel H est normal.*

Proposition 1.17. *Soit H un sous-groupe de G. Les assertions suivantes sont équivalentes :*

(1) H est un sous-groupe normal de G,

(2) H est stable par tout automorphisme intérieur,

(3) Pour tout $g \in G$, on a $gHg^{-1} = H$,

(4) H est le noyau d'un morphisme de groupes.

Si H vérifie l'une de ces conditions, on dit que H est distingué dans G.

Démonstration. Les implications $(4) \Rightarrow (1) \Rightarrow (2) \Rightarrow (3)$ sont immédiates (par définition). Il reste à prouver que (3) implique (4). On sait que H agit sur G par multiplication à droite. On considère l'application $\psi : G \to G/H$ donnée par $g \mapsto gH$.

On voit que G/H est un groupe d'élément neutre H. On observe alors que ψ est un morphisme de groupes car

$$\psi(g)\psi(g') = gHg'H = g(Hg')H = g(g'H)H = (gg')H = \psi(gg').$$

On obtient finalement

$$\mathrm{Ker}(\psi) = \{g \in G \mid gH = H\} = H,$$

et H est bien le noyau d'un morphisme de groupes. □

On a les propriétés générales suivantes :

Proposition 1.18. *(1) Tout sous-groupe d'indice 2 est distingué (même si G est infini).*

(2) Plus généralement, si p est le plus petit nombre premier qui divise l'ordre d'un groupe fini G alors tout sous-groupe d'indice p de G est distingué.

(3) Si $\varphi : G \to H$ est un morphisme de groupes et K est un sous-groupe distingué de H, alors $\varphi^{-1}(K)$ est distingué dans G.

Démonstration. (1) Soit H un sous-groupe de G d'indice 2. Il y a deux classes à gauche : H et le complément H^c de H dans G. On peut donc écrire $H^c = gH$ pour un g dans G. L'application $f : g \mapsto g^{-1}$ est une bijection de G dans lui-même telle que $f(H) = H$ donc on a aussi $f(H^c) = H^c$. on obtient $Hg^{-1} = gH$. Mais Hg^{-1} est une classe à droite contenant g donc c'est Hg. On a finalement $gH = Hg$ et H est bien distingué dans G.

(2) Supposons G fini. Notons p le plus petit diviseur premier de $|G|$ et on suppose qu'il existe un sous groupe H de G d'indice p. On considère l'action φ de G sur G/H : pour tout g de G et toute classe xH dans G/H, on a $\varphi(g)(xH) = gxH$. En particulier, on a $\mathrm{Ker}(\varphi) \subset H$ et donc $|\mathrm{Ker}(\varphi)|$ divise $|H|$.

Comme on a $G/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi) \subset \mathrm{Bij}(G/H) \simeq \mathfrak{S}_p$, en passant au cardinal, on obtient que $\frac{|G|}{|\mathrm{Ker}(\varphi)|}$ divise $p!$. Puisque p est le plus petit diviseur premier de $|G|$, on obtient que $\frac{|G|}{p}$ divise $|\mathrm{Ker}(\varphi)|$. Mais on a aussi $\frac{|G|}{p} = |H|$. D'où $|H|$ divise $|\mathrm{Ker}(\varphi)|$ et on voit finalement que $H = \mathrm{Ker}(\varphi)$. Le sous-groupe H est donc bien distingué dans G.

(3) Exercice. □

Exemple 1.19. (1) Le sous-groupe $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$.

(2) L'image directe d'un sous-groupe distingué n'est pas un sous-groupe distingué en général : considérons par exemple, le morphisme de groupes injectif $j : \mathbf{Z}/2\mathbf{Z} \to \mathfrak{S}_3$ tel que $j(1) = (1, 2)$.

(•) **Quotients de groupe.**

Si H est un sous-groupe distingué de G alors l'espace quotient G/H est naturellement muni d'une structure de groupe et on a un morphisme naturel de groupes

$$\pi_H : G \to G/H$$

donné par $\pi_H(g) = gH$ et de noyau H.

Le morphisme $\pi_H : G \to G/H$ satisfait la propriété universelle suivante : pour tout morphisme de groupes $f : G \to G'$ tel que $H \subset \mathrm{Ker}(f)$, il existe un unique morphisme de groupes $\overline{f} : G/H \to G'$ tel que $\overline{f} \circ \pi_H = f$. Le morphisme $\overline{f}$ est obtenu en posant $\overline{f}(gH) := f(g)$. On vérifie aisément que la définition ne dépend pas du choix du représentant g et qu'on obtient de cette façon un morphisme de groupe.

Proposition 1.20. *Si $f : G \to G'$ est un morphisme de groupes alors $\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ est un isomorphisme de groupes.*

Démonstration. Exercice. □

Proposition 1.21. *Si H, K sont deux sous-groupes de G avec H distingué dans G alors $H \cap K$ est distingué dans K et*

$$HK/H \simeq K/(H \cap K).$$

Démonstration. On considère le morphisme de groupes $\pi_H : G \to G/H$. Alors

$$\mathrm{Im}(\pi_H|_K) = KH/H \quad \text{ et } \mathrm{Ker}(\pi_H|_K) = H \cap K.$$

Ainsi $H \cap K$ est distingué dans K (c'est un noyau) et $\pi_H|_K$ induit l'isomorphisme $HK/H \simeq K/(H \cap K)$. □

Exemple 1.22 (Sous-groupe dérivé et groupe résoluble)**.** Le sous-groupe dérivé $\mathcal{D}(G)$ d'un groupe G est le sous-groupe de G engendré par les commutateurs d'éléments de G (i.e. les éléments $[x, y] := x^{-1}y^{-1}xy$ avec x et y dans G. On a alors

Proposition 1.23. *Le groupe dérivé $\mathcal{D}(G)$ est le plus petit sous-groupe distingué de G tel que $G/\mathcal{D}(G)$ est abélien.*

Démonstration. Notons $G' := G/\mathcal{D}(G)$. On a $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$ donc $\mathcal{D}(G)$ est bien un sous-groupe distingué de G. Pour u et v dans G' représentés par les éléments x et y dans G, on a

$$[u, v] = [\pi_{\mathcal{D}(G)}(x), \pi_{\mathcal{D}(G)}(y)] = \pi_{\mathcal{D}(G)}([x, y]) = 1_{G'}.$$

Ainsi, G' est abélien.

Soit maintenant H un sous-groupe distingué de G tel que G/H est abélien. On veut montrer que H contient $\mathcal{D}(G)$ et pour cela, il suffit de montrer que pour tout x et y de G, le commutateur $[x, y]$ est dans H. Mais on a

$$\pi_H([x, y]) = [\pi_H(x), \pi_H(y)] = 1_{G/H}$$

car, par hypothèse, le groupe G/H est commutatif. Ainsi $[x, y]$ est bien dans H. □

On dit qu'un groupe est *résoluble* s'il existe une suite finie $(H_i)_{0\leq i\leq n}$ de sous-groupes distingués H_i de G telle que $H_0 = G$ et $H_n = \{1_G\}$ et pour tout i de $[|1, n|]$, le groupe H_i est un sous-groupe distingué de H_{i-1} et le quotient H_{i-1}/H_i est abélien. Une telle suite est parfois appelée suite de résolubilité.

On appelle suite dérivée de G, la suite de sous-groupes $(H_i)_{i\in\mathrm{N}}$ de G définie par récurrence par $H_0 := G$ et pour tout $n \geq 1$, $H_n := \mathcal{D}(H_{n-1})$. On peut alors montrer le résultat suivant (exercice) :

Proposition 1.24. *Un groupe G est résoluble si et seulement si sa suite dérivée est une suite de résolubilité.*

1.3 Les p-groupes

Soit p un nombre premier fixé. Un p-groupe fini est un groupe d'ordre une puissance de p. Le plus simples est $\mathbf{Z}/p\mathbf{Z}$. Un autre exemple est donné par le sous-groupe $\mathrm{UT}_n(\mathbf{F}_p)$ de $\mathrm{GL}_n(\mathbf{F}_p)$ formé des matrices de la forme $\mathrm{Id} + T$ avec T une matrice strictement triangulaire. On a en effet $|\mathrm{UT}_n(\mathbf{F}_p)| = p^{\frac{n(n-1)}{2}}$.

Lemme 1.25. *Soit G un p-groupe fini agissant sur un ensemble fini X. Alors*

$$|X^G| = |X| \bmod p.$$

Démonstration. On fixe $(x_i)_{i\in I}$ une famille de représentants pour l'action de G sur X. Notons $|G| = p^n$. On sait que $|\mathrm{Stab}_G(x_i)|$ divise p^n donc est de la forme p^{ℓ_i} avec $\ell \leq n$. Si $\ell_i < n$, on obtient donc

$$\frac{|G|}{|\mathrm{Stab}_G(x_i)|} = 0 \bmod p.$$

Ainsi, la formule des classes donne

$$|X| = \sum_{i\in I} \frac{|G|}{|\mathrm{Stab}_G(x_i)|} = \sum_{\ell_i=n} 1 \bmod p.$$

Or, si $\ell_i = n$, alors x_i est un point fixe pour G. Il suit :

$$\sum_{\ell_i=n} 1 = |X^G|$$

et on obtient le résultat voulu. □

Proposition 1.26. *Soit G un p-groupe fini. Alors $\mathcal{Z}(G)$ est non-trivial.*

Démonstration. Considérons l'action de G sur lui-même par conjugaison. L'ensemble des points fixes est $\mathcal{Z}(G)$. Par le lemme ci-dessus on a donc

$$|\mathcal{Z}(G)| = |G| = 0 \bmod p.$$

Puisque $\mathcal{Z}(G)$ contient le neutre il est de cardinal plus grand que 1 et puisque $1 \neq 0 \bmod p$, il existe nécessairement un élément non trivial dans $\mathcal{Z}(G)$. □

Remarque 1.27. De manière similaire, on peut montrer que si G est un p-groupe agissant de manière linéaire (i.e. les $\varphi(g)$ sont linéaires) sur un $\mathbf{F}_p$-espace vectoriel E de dimension finie ≥ 1 alors E^G est non-trivial.

Théorème 1.28 (Théorème de Cauchy)**.** *Un groupe fini G d'ordre divisible par p contient un élément d'ordre p.*

Démonstration. Soit X l'ensemble des p-uplets $(g_0, \ldots, g_{p-1})$ d'éléments de G tels que $g_0 \cdots g_{p-1} = 1_G$. L'application de X dans G^{p-1} obtenue en oubliant g_0 est alors une bijection. Il suit que le cardinal de X est divisible par p.

On fait maintenant agir $\mathbf{Z}/p\mathbf{Z}$ sur X via la formule

$$\overline{x} \cdot (g_0, \ldots, g_{p-1}) = (g_x, g_{x+1} \ldots, g_0, \ldots, g_{x-1})$$

où x est un représentant de x dans $\{0, \cdots, p-1\}$. On applique le lemme ci-dessus et on obtient

$$|X^{\mathbf{Z}/p\mathbf{Z}}| = |X| = 0 \bmod p.$$

L'ensemble $X^{\mathbf{Z}/p\mathbf{Z}}$ n'est donc pas trivial et il existe un élément non trivial $z := (g_0, \cdots, g_{p-1})$ fixé par $\mathbf{Z}/p\mathbf{Z}$. En considérant son image par l'élément $\overline{1}$ de $\mathbf{Z}/p\mathbf{Z}$, on obtient

$$g_0 = g_1 = \cdots = g_{p-1}.$$

L'élément z de X est donc de la forme $(g, \cdots g)$ avec $g \neq 1_G$ et on a $g^p = 1_G$ par définition de X. □

Théorème 1.29 (Théorème de Sylow)**.** *Soit G un groupe fini et p un nombre premier divisant l'ordre de G. On écrit $|G| = p^\alpha m$ avec m premier à p. Alors*

(1) G admet des sous-groupes d'ordre p^α, on les appelle p-(sous-groupes de) Sylow de G,

(2) les p-Sylow sont deux à deux conjugués,

(3) si n_p est le nombre de p-Sylow de G alors $n_p = 1 \bmod p$ et n_p divise m.

Exemple 1.30. L'ordre du groupe $\mathrm{GL}_n(\mathbf{F}_p)$ est égal à $p^{\frac{n(n-1)}{2}}(p^n-1)\cdots(p-1)$. Le groupe $\mathrm{UT}_n(\mathbf{F}_p)$ est un p-Sylow de $\mathrm{GL}_n(\mathbf{F}_p)$.

Preuve du théorème 1.29. On commence par montrer les lemmes suivants :

Lemme 1.31. *Soit G un groupe fini d'ordre n et k un corps quelconque. Alors G est isomorphe à un sous-groupe de $\mathrm{GL}_n(k)$.*

Preuve du Lemme 1.31. C'est une conséquence du théorème de Cayley (Proposition 1.11). On sait que G est isomorphe à un sous-groupe de $\mathfrak{S}_n$. Pour n'importe quel corps k, on a un morphisme injectif $\mathfrak{S}_n \to \mathrm{GL}_n(k)$ donné par $\sigma \mapsto M_\sigma$ où

$$(M_\sigma)_{i,j} = \begin{cases} 1 & \text{si } i = \sigma(j) \\ 0 & \text{sinon.} \end{cases}$$

Par composition, on obtient un morphisme injectif $G \to \mathrm{GL}_n(k)$. □

Lemme 1.32. *Soit G un groupe fini. On considère H un sous-groupe de G et p un facteur premier de l'ordre de H. Supposons que G contient un p-Sylow P. Alors H contient un p-sous-groupe de Sylow de la forme $H \cap gPg^{-1}$ pour un g dans G.*

Démonstration. Le groupe H agit sur G/P par multiplication à gauche. Puisque P est maximal, le cardinal de G/P n'est pas divisible par p. Il existe donc une orbite $\mathcal{O}$ de l'action de H sur G/P tel que le cardinal de $\mathcal{O}$ n'est pas divisible par p. On écrit $\mathcal{O} = H \cdot \overline{g}$ pour un $\overline{g}$ dans G/P. On a

$$\begin{aligned} \mathrm{Stab}(\overline{g}) &= \{h \in H \mid h\overline{g} = \overline{g}\} \\ &= \{h \in H \mid hgP = gP\} \\ &= \{h \in H \mid g^{-1}hg \in P\} \\ &= \{h \in H \mid h \in gPg^{-1}\} = H \cap gPg^{-1}. \end{aligned}$$

Comme on a $|gPg^{-1}| = |P|$, on voit que gPg^{-1} est encore un p-Sylow de G. Comme $\mathrm{Stab}(\overline{g})$ est un sous-groupe de gPg^{-1}, c'est un p-groupe. On a donc

$$|H| = |\mathrm{Stab}(\overline{g})| \cdot \mathrm{card}(\mathcal{O})$$

avec $|\mathrm{Stab}(\overline{g})|$ égal à une puissance de p et $\mathrm{card}(\mathcal{O})$ premier à p. Donc $|\mathrm{Stab}(\overline{g})|$ est un p-Sylow de H. □

On peut maintenant prouver le théorème 1.29]. On commence par monter le point (1). Si on note $n = p^\alpha m$ l'ordre de G alors par le lemme 1.31, le groupe G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{F}_p)$. Mais $\mathrm{GL}_n(\mathbf{F}_p)$ contient le p-Sylow $\mathrm{UT}_n(\mathbf{F}_p)$ (Exemple 1.30). Par le lemme 1.32, G admet donc lui-même un p-Sylow.

Pour montrer le point (2), on applique le lemme 1.32 à un p-Sylow P de G (il existe par (1)) : si on considère S un autre p-Sylow de G alors S contient un p-Sylow $S \cap gPg^{-1}$. Par hypothèse S est un p-groupe donc $S \cap gPg^{-1} = S$, i.e. $S \subset gPg^{-1}$. Mais S et gPg^{-1} sont tous les deux des p-Sylow de G donc ils ont le même ordre, d'où $S = gPg^{-1}$.

Montrons maintenant le point (3). Soit P un p-Sylow de G. Le groupe P agit sur l'ensemble des p-Sylow de G par conjugaison. Notons X cet ensemble ; son cardinal est donc n_p. Par le lemme 1.25, on a

$$n_p = |X^P| \bmod p.$$

On va montrer que $X^P = \{P\}$. Soit S dans X tel quel pour tout g de P, on a $gSg^{-1} = S$. Considérons le groupe $G_0 := PS$. Les groupes P et S sont des p-Sylow de G_0 : ils sont des p-groupes contenus dans G_0 et leur ordre est maximal dans G_0 puisqu'il l'est déjà dans G. On applique le point (2) au groupe G_0 : les p-Sylow P et S sont conjugués dans $G_0 = PS$. Donc il existe un élément gs dans PS tel que

$$P = (gs)S(gs)^{-1} = g(sSs^{-1})g^{-1} = gSg^{-1} = S$$

où la dernière égalité vient de notre hypothèse sur S. On a donc bien $X^P = \{P\}$ et en particulier, $n_p = 1 \bmod p$.

Enfin, si on considère l'action de G par conjugaison sur l'ensemble de ses sous-groupes, tous les p-Sylow sont dans la même orbite par le point (2). Par l'équation aux classes, on a donc $n_p = [G : \mathrm{Stab}_G(P)]$ et donc n_p divise n. On vient de voir que n_p et p sont premiers entre eux : ceci implique que n_p divise m, comme souhaité.

□

1.4 Groupes finis usuels

(•) Groupes cycliques.

Un groupe monogène est un groupe engendré par un élément. Il peut être soit infini et dans ce cas, il est isomorphe au groupe $(\mathbf{Z}, +)$, soit fini et il est alors isomorphe au groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ pour un n dans N^*. On notera C_n le groupe monogène d'ordre n. On appelle groupe cyclique tout groupe isomorphe à C_n.

Les groupes monogènes satisfont les propriétés suivantes (exercice) :

(1) Les sous-groupes de $\mathbf{Z}$ sont les groupes de la forme $d\mathbf{Z}$ avec d dans N. Ceux de $\mathbf{Z}/n\mathbf{Z}$ sont de la forme $d\mathbf{Z}/n\mathbf{Z}$ avec d divise n.

(2) Les générateurs de $\mathbf{Z}/n\mathbf{Z}$ sont les classes $k + n\mathbf{Z}$ avec k premier à n. Autrement dit, ce sont les inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$.

(3) Les automorphismes de $\mathbf{Z}/n\mathbf{Z}$ sont les morphismes de la forme $x \mapsto \lambda x$ avec λ inversible de $\mathbf{Z}/n/\mathbf{Z}$.

Exemple 1.33 (Groupe des racines de l'unité)**.** Si K est un corps, on définit le groupe des racines de l'unité :

$$\mu_n(K) := \{x \in K^\times \mid x^n = 1\}$$

qui est un sous-groupe de $K^\times$. Alors $\mu_n(K)$ est un groupe cyclique d'ordre divisant n. Si $K = \mathbf{C}$, on voit également que $\mu_n(\mathbf{C})$ est un sous-groupe du groupe $\mathbf{U}$ des nombres complexes de module 1. Le groupe $\mathbf{U}$ est un groupe topologique compact. On peut montrer qu'en fait, tout sous-groupe discret de $\mathbf{U}$ est isomorphe à un $\mu_n(\mathbf{C})$.

Rappelons la notion de *groupe dual* :

Définition 1.34. Soit G un groupe. Un caractère (abélien) est un morphisme de groupes $\chi : G \to \mathbf{C}^*$. Le groupe dual de G, noté $\widehat{G}$, est le groupe abélien formé par ses caractères.

On a alors

Proposition 1.35. *Le groupe dual de $\mathbf{Z}/n\mathbf{Z}$ est canoniquement isomorphe à $\mu_n(\mathbf{C})$ (lui-même isomorphe à $\mathbf{Z}/n\mathbf{Z}$).*

Démonstration. L'isomorphisme est donné par

$$\begin{cases} \widehat{\mathbf{Z}/n\mathbf{Z}} \to \mu_n(\mathbf{C}) \\ \chi \mapsto \chi(\overline{1}) \end{cases}$$

En effet, on doit avoir

$$\chi(\overline{1})^n = \chi(\overline{n}) = \chi(0) = 1$$

donc il est bien défini et c'est évidemment un morphisme de groupe. Réciproquement pour toute racine n-ième de l'unité ζ, on peut définir un unique χ tel que $\chi(\overline{1}) = \zeta$ en envoyant k sur ζ^k. □

(•) Structure des groupes abéliens finis.

Commençons par rappeler le résultat suivant :

Lemme 1.36. *Soit G un groupe abélien fini. Alors il existe dans G un élément d'ordre égal à l'exposant de G (c'est-à-dire au* ppcm *des ordres des éléments de G).*

Démonstration. On montre d'abord que pour tous x, y dans G d'ordres respectifs m et n premiers entre eux, le produit xy est d'ordre $m \cdot n$. On a évidemment

$$(xy)^{mn} = 1$$

donc l'ordre de xy divise mn. Soit maintenant $k \geq 1$ tel que $(xy)^k = 1$. En élevant à la puissance n, on obtient

$$x^{kn} = 1,$$

donc m divise kn. Puisque m et n sont premiers entre eux, m divise k. Par symétrie, on a aussi que n divise k, donc mn divise k. On obtient finalement que xy est d'ordre mn.

On décompose l'exposant de G en facteurs premiers :

$$\exp(G) = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

avec les p^i nombres premiers distincts. Par définition de l'exposant de G, pour tout $1 \leq i \leq r$, il existe g_i dans G dont l'ordre est divisible par $p_i^{\alpha_i}$. Notons $p_i^{\alpha_i} m_i$ l'ordre de g_i. Alors $g_i^{m_i}$ est d'ordre $p_i^{\alpha_i}$ et on a vu qu'alors l'élément

$$g := g_1^{m_1} \cdots g_r^{m_r}$$

est d'ordre exactement $p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \exp(G)$. □

On a le théorème :

Théorème 1.37. *Soit G un groupe abélien fini non trivial. Il existe un entier $r \geq 1$ et des entiers $n_1, \ldots, n_r \geq 2$ avec n_{i+1} divise n_i pour tout $1 \leq i \leq r-1$, tels que*

$$G \simeq \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}.$$

Plus généralement si G est un groupe abélien de type fini, alors il existe un entier $\ell \geq 0$, un entier $r \geq 1$ et des entiers $n_1, \ldots, n_r \geq 2$ avec n_{i+1} divise n_i pour tout $1 \leq i \leq r-1$, tels que

$$G \simeq \mathbf{Z}^\ell \times \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}.$$

(•) **Groupes de permutations.**

Soit n un entier plus grand que 2. On note $\mathfrak{S}_n$ le groupe des permutations de $[|1, n|]$, appelé groupe symétrique. On note $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ la signature. Rappelons que la signature est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\{\pm 1\}$. On note $\mathfrak{A}_n$ son noyau, appelé groupe alterné.

On rappelle de plus les résultats suivants :

(1) Tout σ de $\mathfrak{S}_n$ se factorise en un produit de cycles deux à deux disjoints (et la décomposition est unique à l'ordre des facteurs près).

(2) Les transpositions engendrent $\mathfrak{S}_n$. L'ensemble $\{(1, i),\ 1 \leq i \leq n\}$ engendre $\mathfrak{S}_n$. Le nombre minimal de transpositions engendrant $\mathfrak{S}_n$ est $n - 1$.

(3) $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$. Il est engendré par les 3-cycles pour $n \geq 3$. On verra en TD que pour $n \geq 5$, il est simple (c'est-à-dire que ses seuls sous-groupes sont $\{e\}$ et lui-même). Si $n = 4$, le groupe $\mathfrak{A}_4$ est d'ordre 12 et le sous-groupe

$$\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

est distingué.

(4) En écrivant $\sigma = \sigma_1 \dots \sigma_n$ comme un produit de cycles disjoints rangés par ordre de longueur décroissant, on construit une application φ de $\mathfrak{S}_n$ dans l'ensemble des partitions de n en posant $\varphi(\sigma_n) := (\ell(\sigma_1), \dots, \ell(\sigma_n))$. Alors pour tout σ, τ dans $\mathfrak{S}_n$, on a $\varphi(\tau\sigma\tau^{-1}) = \varphi(\sigma)$ et on obtient :

Théorème 1.38. *L'application φ induit une bijection de l'ensemble des classes de conjugaison de $\mathfrak{S}_n$ sur celui des partitions de n*

2 Anneaux via des exemples

Rappelons qu'on a les implications :

$$\begin{cases} \text{euclidien} \Rightarrow \text{principal} \Rightarrow \text{factoriel} \Rightarrow \text{intégralement clos} \\ \text{principal} \Rightarrow \text{noethérien} \Rightarrow \text{tout élément est produit d'irréductibles} \end{cases}$$

2.1 Exemples d'anneaux d'entiers

(•) **Anneaux euclidiens.** Les anneaux $\mathbf{Z}[i]$ et $\mathbf{Z}[i\sqrt{2}]$ sont euclidiens.

Démonstration. Plus généralement, on va montrer que pour tout d dans $\{-2,-1,0,1,2,3\}$, l'anneau $\mathbf{Z}[\sqrt{d}]$ est euclidien pour le stathme $|N|$, où N désigne la norme multiplicative

$$N : a+b\sqrt{d} \in \mathbf{Q}[\sqrt{d}] \mapsto a^2 - db^2 = (a-b\sqrt{d})(a+b\sqrt{d}) \in \mathbf{Q}.$$

Soient x et y dans $\mathbf{Z}[\sqrt{d}]$. On veut écrire

$$x = qy + r \quad \text{avec} \quad q = \alpha + \beta\sqrt{d} \in \mathbf{Z}[\sqrt{d}] \text{ et } |N|(r) < |N|(y).$$

Écrivons $\frac{x}{y} = a + b\sqrt{d}$ dans $\mathbf{Q}[\sqrt{d}]$. Si $|d| < 3$, on peut choisir (α, β) dans $\mathbf{Z} \times \mathbf{Z}$ tels que

$$|N|(\frac{x}{y} - q) = |N|((a+b\sqrt{d}) - (\alpha+\beta\sqrt{d})) < 1. \tag{2.1.1}$$

En effet, si on prend α et β entiers tels que

$$|a-\alpha| \leq \frac{1}{2} \text{ et } |b-\beta| \leq \frac{1}{2},$$

on obtient

$$|N|((a+b\sqrt{d})-(\alpha+\beta\sqrt{d})) = \big||a-\alpha|^2 - d|b-\beta|^2\big| \leq |a-\alpha|^2 + |d|\cdot|b-\beta|^2 \leq (\frac{1}{2})^2 + |d|(\frac{1}{2})^2 = \frac{1+|d|}{4} < 1.$$

Si $d = 3$, on a encore

$$\big||a-\alpha|^2 - 3|b-\beta|^2\big| \leq \max(|a-\alpha|^2, 3|b-\beta|^2) \leq \max\Big((\frac{1}{2})^2, 3\cdot(\frac{1}{2})^2\Big) = \frac{3}{4} < 1.$$

Dans tous les cas, on a bien (2.1.1). Posons $r := x - qy$. On obtient

$$|N|(r) = |N|(x-qy) = |N|(y)\cdot|N|(\frac{x}{y} - q) < |N|(y),$$

comme attendu. □

(•) **Noethérien n'implique pas intégralement clos.** L'anneau $\mathbf{Z}[i\sqrt{3}]$ est noethérien non intégralement clos.

Démonstration. On a $\mathbf{Z}[i\sqrt{3}] \simeq \mathbf{Z}[X]/\langle X^2+3\rangle$. Puisque $\mathbf{Z}$ est noethérien, l'anneau $\mathbf{Z}[X]$ l'est aussi et donc $\mathbf{Z}[i\sqrt{3}]$ est lui-même noethérien en tant que quotient d'un anneau noethérien.

Pour voir qu'il n'est pas intégralement clos, on peut considérer l'élément

$$z := \frac{1+i\sqrt{3}}{2} \in \mathbf{Q}(i\sqrt{3}) = \mathrm{Frac}(\mathbf{Z}[i\sqrt{3}]).$$

On vérifie facilement que z n'appartient pas à $\mathbf{Z}[i\sqrt{3}]$ mais qu'il est racine du polynôme $X^2 - X + 1$ de $\mathbf{Z}[i\sqrt{3}][X]$. □

(•) **Noethérien n'implique pas factoriel.** L'anneau $\mathbf{Z}[i\sqrt{5}]$ est noethérien non factoriel.

Démonstration. Comme précédemment, on a $\mathbf{Z}[i\sqrt{5}] \simeq \mathbf{Z}[X]/\langle X^2+5\rangle$ et donc $\mathbf{Z}[i\sqrt{5}]$ est bien noethérien comme quotient d'un anneau noethérien.

Rappelons que dans un anneau factoriel, tous les éléments irréductibles sont aussi premiers. Ainsi, pour montrer que $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel, on va montrer que l'élément $3 \in \mathbf{Z}[i\sqrt{5}]$ est irréductible sans être premier. Pour voir qu'un élément est irréductible dans un anneau d'entiers, on utilise généralement la norme multiplicative :

$$N : a + bi\sqrt{5} \in \mathbf{Z}[i\sqrt{5}] \mapsto a^2 + 5b^2 \in \mathbf{Z}.$$

Écrivons $3 = xy$ dans $\mathbf{Z}[i\sqrt{5}]$ et appliquons $N(-)$. On obtient

$$9 = N(x)N(y) \quad \text{avec } N(x), N(y) \in \mathbf{Z}.$$

En écrivant les équations, on voit facilement que $N(-)$ ne peut pas prendre les valeurs ± 3. On en déduit :

$$N(x) = \pm 1 \quad \text{ou} \quad N(y) = \pm 1.$$

Mais une relation de la forme $(a+bi\sqrt{5})(a-bi\sqrt{5}) = \pm 1$ implique que $(a+bi\sqrt{5})$ et $(a-bi\sqrt{5})$ sont inversibles dans l'anneau $\mathbf{Z}[i\sqrt{5}]$. Ainsi soit x, soit y est bien inversible dans $\mathbf{Z}[i\sqrt{5}]$ et on obtient finalement que 3 est irréductible.

Montrons qu'il n'est pas premier. Pour cela, il suffit de considérer le quotient

$$\mathbf{Z}[i\sqrt{5}]/\langle 3\rangle \simeq (\mathbf{Z}[X]/\langle X^2+5\rangle)/\langle 3\rangle \simeq (\mathbf{Z}[X]/\langle 3\rangle)/\langle X^2+5\rangle \simeq \mathbf{F}_3[X]/\langle (X-1)(X+1)\rangle,$$

où le deuxième isomorphisme suit du résultat général (pour $I = \langle X^2+5\rangle$ ou $I = \langle 3\rangle$ et $J = \langle X^2+5, 3\rangle$) :

Proposition 2.1 (Troisième théorème d'isomorphisme pour les anneaux)**.** *Soit A un anneau, et I et J des idéaux de A tels que $I \subset J \subset A$. Alors J/I est un idéal de A/I et l'application naturelle induit un isomorphisme d'anneaux :*

$$(A/I)/(J/I) \simeq A/J.$$

On voit que l'anneau obtenu est non-intègre.

Un autre solution pour voir que $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel est de considérer les décompositions

$$3 \times 3 = (2 - i\sqrt{5}) \times (2 + i\sqrt{5}) \quad \text{ou} \quad 3 \times 7 = (4 - i\sqrt{5}) \times (4 + i\sqrt{5}),$$

qui contredisent l'unicité de la décomposition en éléments irréductibles. □

2.2 Exemples d'anneaux de polynômes

(•) L'anneau $K[X, Y]/\langle X^2 - Y\rangle$ est euclidien.

Démonstration. Il suffit de montrer que $K[X, Y]/\langle X^2 - Y\rangle$ est isomorphe à $K[X]$ car l'anneau de polynômes $K[X]$ est euclidien (relativement au degré polynômial usuel). Un isomorphisme s'obtient en factorisant le morphisme d'anneaux surjectif de $K[X, Y]$ dans $K[X]$ envoyant un polynôme $P(X, Y)$ sur $P(X, X^2)$. On vérifie que le noyau de ce morphisme est $(Y - X^2)K[X, Y]$. En effet, écrivons la division euclidienne d'un polynôme $P(X, Y)$ de $K[X, Y]$ par le polynôme unitaire $Y - X^2$ de $K[X][Y]$, on obtient

$$P(X, Y) = (Y - X^2)Q(X, Y) + R(X), \quad \text{avec} \quad Q(X, Y) \in K[X, Y] \text{ et } R[X] \in K[X].$$

On voit donc que $Y - X^2$ divise $P(X, Y)$ dans $K[X, Y]$ si et seulement si $R(X) = P(X, X^2)$ est nul. □

(•) L'anneau $K[X, Y]/\langle XY - 1\rangle$ est euclidien.

Démonstration. Il suffit de montrer qu'on a un isomorphisme

$$K[X, Y]/\langle XY - 1\rangle \simeq K[X, \frac{1}{X}],$$

car l'anneau de fractions $K[X, 1/X]$ est euclidien (relativement au degré donné par $\deg(P\big(\frac{1}{X}\big) + Q(X)) = \deg(P) + \deg(Q)$). Un tel isomorphisme peut s'obtenir en factorisant le morphisme d'anneaux surjectif

$$P \in K[X, Y] \mapsto P(X, \frac{1}{X}) \in K[X, \frac{1}{X}].$$

On va montrer que son noyau est bien $(XY-1)K[X,Y]$. En effet, si $P(X,Y)=\sum_{k=0}^{n}P_k(X)Y^k$ et $Q(X,Y)=\sum_{k=0}^{n-1}Q_k(X)Y^k$ avec $P_k,Q_k\in K[X]$, alors $P=(XY-1)Q$ si et seulement si

$$\begin{aligned}&P_n=XQ_{n-1},\\&P_k=XQ_{k-1}-Q_k\quad\text{ si } 0<k<n,\\&P_0=-Q_0.\end{aligned}$$

On obtient

$$\begin{cases}Q_k=-\sum_{\ell=0}^{k}X^{k-\ell}P_\ell\quad\text{ si } 0\leq k\leq n-1,\\XQ_{n-1}=P_n\end{cases}. \tag{2.2.1}$$

Or si $P(X,\frac{1}{X})=0$, alors

$$P_n+\sum_{\ell=0}^{n-1}X^{n-\ell}P_\ell=0,$$

et le système (2.2.1) a bien une solution. En conclusion, on a donc $(XY-1)$ divise $P(X,Y)$ dans $K[X,Y]$ si et seulement si $P(X,\frac{1}{X})=0$ dans $K(X)$. □

(•) L'anneau $K[X,Y]/\langle Y^2-X^3\rangle$ est noethérien non factoriel (et même non intégralement clos).

Démonstration. Montrons d'abord qu'on a un isomorphisme :

$$K[X,Y]/\langle Y^2-X^3\rangle\simeq K+Z^2K[Z](=\{P\in K[Z]\mid P'(0)=0\}).$$

Pour simplifier les notations, appelons A l'anneau $K+Z^2K[Z]$. On considère le morphisme d'anneaux surjectif :

$$P\in K[X,Y]\mapsto P(Z^2,Z^3)\in A.$$

Comme précédemment, on montre que son noyau est $(Y^2-X^3)K[X,Y]$: en écrivant P et Q comme dans l'exemple précédent, on voit que $P=(Y^2-X^3)Q$ si et seulement si

$$\begin{aligned}&P_n=XQ_{n-2},\\&P_{n-1}=Q_{n-3},\\&P_k=Q_{k-2}-X^3Q_k\quad\text{ si } 2\leq k\leq n-2,\\&P_1=-X^3Q_1,\\&P_0=-X^3Q_0,\end{aligned}$$

ce qui donne

$$\begin{cases}Q_k=\sum_{0\leq\ell\leq\frac{(n-k-2)}{2}}X^{3\ell}P_{2k+2\ell+2}\quad\text{ si } 0\leq k\leq n-2,\\\sum_{0\leq\ell\leq\frac{n}{2}}X^{3\ell}P_{2\ell}=0,\\\sum_{0\leq\ell\leq\frac{n-1}{2}}X^{3\ell}P_{2\ell+1}=0.\end{cases} \tag{2.2.2}$$

On note F et G les polynômes de $K[X,Y]$ tels que $P(X,Y) = F(X,Y^2) + YG(X,Y^2)$ (parties paire et impaire de P relativement au degré de Y), i.e.

$$F(X,Y^2) = \frac{P(X,Y) + P(X,-Y)}{2} \quad \text{et} \quad G(X,Y^2) = \frac{P(X,Y) - P(X,-Y)}{2Y}$$

et on observe que le système (2.2.2) admet une solution si et seulement si $F(X,X^3) = G(X,X^3) = 0$. On conclut en utilisant l'équivalence :

$$F(X,X^3) = G(X,X^3) = 0 \Leftrightarrow F(Z^2,Z^6) = G(Z^2,Z^6) = 0 \Leftrightarrow P(Z^2,Z^3) = 0.$$

Pour terminer, il reste à voir que A est intègre, noethérien mais non intégralement clos. Il est intègre comme sous-anneau de $K[Z]$ lui-même intègre et il est noethérien car isomorphe à un quotient de $K[X,Y]$ qui est noethérien. Pour voir qu'il n'est pas intégralement clos, on peut considérer l'élément $\alpha := \frac{Z^3}{Z^2} \in \mathrm{Frac}(A) \setminus A$ qui satisfait l'équation $\alpha^2 - Z^2 = 0$.

En particulier, on obtient ainsi que l'anneau A n'est pas non plus factoriel.

□

(•) Si -1 est un carré dans le corps K, les anneaux $K[X,Y]/\langle X^2 + Y^2 + 1\rangle$ et $K[X,Y]/\langle X^2 + Y^2 - 1\rangle$ sont isomorphes et euclidiens.

Démonstration. Si i dans K désigne une racine carrée de -1 alors le changement de variables

$$(U,V) := (X + iY, X - iY) \Rightarrow (X,Y) = \big(\frac{U+V}{2}, \frac{U-V}{2i}\big)$$

induit un morphisme d'anneaux surjectif

$$P \in K[X,Y] \mapsto P\big(\frac{U - \frac{1}{U}}{2}, \frac{U + \frac{1}{U}}{2i}\big) \in K[U, \frac{1}{U}]$$

de noyau $(X^2 + Y^2 + 1)K[X,Y] = (UV + 1)K[U,V]$. On obtient

$$K[X,Y]/\langle X^2 + Y^2 + 1\rangle \simeq K[U, \frac{1}{U}],$$

et $K[X,Y]/\langle X^2 + Y^2 + 1\rangle$ est donc bien euclidien. De la même façon, le morphisme surjectif

$$P \in K[X,Y] \mapsto P\big(\frac{U + \frac{1}{U}}{2}, \frac{U - \frac{1}{U}}{2i}\big) \in K[U, \frac{1}{U}]$$

de noyau $(X^2 + Y^2 - 1)K[X,Y] = (UV - 1)K[U,V]$ donne un isomorphisme

$$K[X,Y]/\langle X^2 + Y^2 - 1\rangle \simeq K[U, \frac{1}{U}].$$

En conclusion, on a bien

$$K[X,Y]/\langle X^2+Y^2+1\rangle \simeq K[X,Y]/\langle X^2+Y^2-1\rangle \simeq K[U,\frac{1}{U}],$$

qui est un anneau euclidien. □

(•) L'anneau $\mathbf{R}[X,Y]/\langle X^2+Y^2+1\rangle$ est non-euclidien.

Démonstration. La preuve se fait en deux étapes.

Étape 1 - On montre que les inversibles de l'anneau $A := \mathbf{R}[X,Y]/\langle X^2+Y^2+1\rangle$ sont les constantes non nulles. Pour cela, on commence par remarquer que tout élément $F(X,Y)$ de A peut être représenté au moyen d'un unique couple de polynômes (P,Q) de $\mathbf{R}[X]\times\mathbf{R}[X]$ tel que

$$F(X,Y) = P(X) + Q(X)Y.$$

En effet, si on considère le reste $R(X,Y)$ le reste la division euclidienne de $F(X,Y)$ par $Y^2+(X^2+1)$ dans $\mathbf{R}[X][Y]$ et qu'on écrit $R(X,Y) = P(X)+Q(X)Y$, on voit qu'on a une équivalence

$$F(X,Y) \in (Y^2+X^2+1)\mathbf{R}[X,Y] \Leftrightarrow P = Q = 0.$$

On est ramené à déterminer à quelle condition les éléments de la forme $P(X)+Q(X)Y$ sont inversibles dans A. On a

$$(P_1(X)+Q_1(X)Y)(P_2(X)+Q_2(X)Y) = 1 \text{ dans } A \Rightarrow \begin{cases} P_1Q_2+Q_1P_2 = 0 \\ P_1P_2-(1+X^2)Q_1Q_2 = 1 \end{cases} \text{ dans } \mathbf{R}[X].$$

On résout le système de droite. En posant

$$c := P_2^2+(1+X^2)Q_2^2$$

on obtient

$$P_2 = cP_1 \text{ et } Q_2 = -cQ_1$$

et il suit

$$1 = P_1P_2-(1+X^2)Q_1Q_2 = c(P_1^2+(1+X^2)Q_1^2).$$

Les polynômes c et $P_1^2+(1+X^2)Q_1^2$ sont donc inversibles dans $\mathbf{R}[X]$: ils sont des constantes non nulles. On vérifie qu'alors la seule possibilité pour (P_1,Q_1) est $Q_1 = 0$ et P_1 est dans $\mathbf{R}^\times$.

Étape 2 - Pour montrer que A n'est pas euclidien, on utilise le lemme suivant :

Lemme 2.2. *Un anneau euclidien R contient toujours un élément $x \neq 0$ qui n'est pas inversible et pour lequel le quotient $R/\langle x\rangle$ est un corps qui est égal à l'image de $\{0\}\cup R^\times$ via le morphisme $R \to R/\langle x\rangle$.*

Démonstration. Notons N le stathme pour lequel R est euclidien. Choisissons x dans le complémentaire de $\{0\} \cup R^\times$ qui minimise N sur cette partie. Si y est dans R alors on peut écrire

$$y = qx + r \quad \text{avec} \quad N(r) < N(x),$$

ce qui, par définition de x, force r à appartenir à $\{0\} \cup R^\times$. Ainsi $R = \langle x \rangle \cup (\langle x \rangle + R^\times)$. En passant au quotient $R/\langle x \rangle$, on obtient que $R/\langle x \rangle$ est un corps et l'application quotient est surjective sur $\{0\} \cup R^\times$. □

Montrons que A n'est pas euclidien. Supposons qu'il l'est. Alors, par le lemme, il existe a tel que $A/\langle a \rangle$ est l'image de $\{0\} \cup A^\times = \mathbf{R}$. L'élément -1 est une somme de carrés dans A et via l'application de réduction $A \to A/\langle a \rangle$, il reste donc une somme de carrés dans $\mathbf{R}$, ce qui n'est pas possible. □

3 Extensions de corps et corps finis

On rappelle qu'un corps est un anneau commutatif K non trivial (contenant donc deux éléments privilégiés : 0 le neutre pour l'addition, et 1 le neutre pour la multiplication) tel que tout élément non nul est inversible. Cela se traduit aussi en termes d'idéaux : un corps est un anneau commutatif K non trivial ayant (0) comme idéal maximal. En particulier, tout morphisme de corps $\varphi : K \to L$ est injectif. On dit que L est une extension de K.

3.1 Extensions de corps : définitions

(•) Caractéristique et degré.

La caractéristique d'un corps K est définie comme le générateur (positif ou nul) du noyau $\mathrm{Ker}(h)$ du morphisme d'anneaux $h : \mathbf{Z} \to K$ défini par $h(1) = 1_K$. Un corps de caractéristique 0 est une extension de $\mathbf{Q}$ et un corps de caractéristique $p \neq 0$ est une extension du corps fini à p éléments, $\mathbf{F}_p$.

Le degré $[K : k]$ d'une extension de corps K/k est la dimension (finie ou infinie) du k-espace vectoriel K. Pour une tour d'extensions $L/K/k$, on a

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

(•) Algébricité et transcendance.

Soit K/k une extension et soit α dans K. Notons φ_α le morphisme (d'anneaux) d'évaluation :

$$\begin{array}{rccc} \varphi_\alpha : & k[X] & \to & K \\ & P & \mapsto & P(\alpha) \end{array}$$

Comme $\mathrm{Im}(\varphi_\alpha)$ est un sous-anneau de K qui est intègre, le noyau de φ_α est un idéal premier de $k[X]$. C'est soit l'idéal nul (0), soit un idéal maximal (P) avec P un polynôme irréductible de $k[X]$. Si $\mathrm{Ker}(\varphi_\alpha) = (0)$, l'élément α est dit *transcendant* sur k. Si $\mathrm{Ker}(\varphi_\alpha) = (P)$ avec P un polynôme irréductible de $k[X]$, l'élément α est dit *algébrique* sur k. Le polynôme P qui engendre $\mathrm{Ker}(\varphi_\alpha)$ est unique si on le choisit unitaire : dans ce cas, on l'appelle le polynôme irréductible de α sur k et on le note $\mathrm{Irr}(\alpha, k)$.

Théorème 3.1. *Soit K/k une extension.*

(i). Soit α dans K algébrique sur k. Alors il existe un polynôme irréductible P de $k[X]$ tel que

$$k[X]/(P) \simeq k(\alpha).$$

De plus $[k(\alpha) : k] = \deg(P) = n$ et $(1, \alpha, \cdots, \alpha^{n-1})$ forme une k-base de $k(\alpha)$. On a ainsi $k(\alpha) = k[\alpha]$, où $k[\alpha] = \{Q(\alpha), Q \in k[X]\}$.

(ii). Soit α dans K transcendant sur k. Alors

$$k(\alpha) \simeq k(X),$$

et $[k(\alpha) : k] = \infty$.

En particulier :

– l'élément α est algébrique sur k si et seulement si l'espace vectoriel $k[\alpha]$ est de dimension finie sur k,

– l'élément α est transcendant sur k si et seulement si aucun polynôme non nul de $k[X]$ ne s'annule en α.

Démonstration. Prouvons le premier point. Puisque α est algébrique sur k, on a $\mathrm{Ker}(\varphi_\alpha) = (P)$ avec P un polynôme irréductible de $k[X]$. Le théorème de factorisation indique que $k[\alpha] = \mathrm{Im}(\varphi_\alpha) \simeq k[X]/(P)$. L'idéal (P) étant maximal, le quotient $k[X]/(P)$ est un corps et il en est de même pour $k[\alpha]$. Par minimalité de $k(\alpha)$, on obtient $k(\alpha) = k[\alpha]$.

Soit n le degré de P. Montrons que la famille $(1, \alpha, \cdots, \alpha^{n-1})$ est une k-base de $k(\alpha)$. On commence par vérifier qu'elle est génératrice. Soit Q dans $k[X]$. Effectuons la division euclidienne de Q par P :

$$Q = PB + R,$$

avec $\deg(R) < n$. Alors $Q(\alpha) = P(\alpha)B(\alpha) + R(\alpha) = R(\alpha)$ et ainsi la famille $(1, \alpha, \cdots, \alpha^{n-1})$ engendre $k[\alpha] = k(\alpha)$ comme k-espace vectoriel.

Montrons que $(1, \alpha, \cdots, \alpha^{n-1})$ est libre. Supposons qu'elle est liée. Il existe un entier $i < n$, des éléments $a_0, \cdots, a_i \in k$ tels que

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

Soit $R = a_iX^i + \cdots + a_1X + a_0 \in k[X]$. La relation précédente indique que $R(\alpha) = 0$ ou encore que $R \in \mathrm{Ker}(\varphi_\alpha) = (P)$. Ainsi P divise R. Comme $\deg(R) < \deg(P)$, alors $R = 0$, ou encore $a_i = \cdots = a_0 = 0$. On a ainsi prouvé que $(1, \alpha, \cdots, \alpha^{n-1})$ forme une base du k-espace vectoriel $k(\alpha)$, ceci conclut la preuve du premier point.

Passons au point *(ii)*. Supposons α transcendant. Alors $\mathrm{Ker}(\varphi_\alpha) = (0)$ et ainsi l'anneau $k[X]$ est isomorphe à $k[\alpha]$, contenu dans $k(\alpha)$. Comme pour tout polynôme non nul $Q \in k[X]$, on a $Q(\alpha) \neq 0$, l'homomorphisme φ_α se prolonge en un homomorphisme injectif φ'_α de $k(X)$ vers $k(\alpha)$. La description suivante :
(3.1.1)

$$k(\{\alpha_1, \cdots, \alpha_n\}) = \Big\{ \frac{P(\alpha_1, \cdots, \alpha_n)}{Q(\alpha_1, \cdots, \alpha_n)} \text{ tel que } P, Q \in k[X_1, \cdots, X_n] \text{ et } Q(\alpha_1, \cdots, \alpha_n) \neq 0 \Big\}.$$

montre ensuite que ce morphisme φ'_α est surjectif et c'est donc un isomorphisme. □

Exemple 3.2. (1) L'élément $\sqrt[3]{2}$ est de degré 3 sur $\mathbf{Q}$. En effet l'élément $\sqrt[3]{2}$ est racine du polynôme $X^3 - 2$ qui est irréductible sur $\mathbf{Q}$ (critère d'Eisenstein appliqué au premier 2), c'est donc le polynôme irréductible de $\sqrt[3]{2}$: $\mathrm{Irr}(\sqrt[3]{2}, \mathbf{Q}) = X^3 - 2$ et $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = \deg(X^3 - 2) = 3$.

(2) Montrons que $[\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}] = 4$. Le corps $\mathbf{Q}(\sqrt{2})$ est un sous-corps de $\mathbf{R}$, ce qui n'est pas le cas de $\mathbf{Q}(i, \sqrt{2})$ (car $i \notin \mathbf{R}$). Ainsi le corps $\mathbf{Q}(i, \sqrt{2})$ contient strictement le corps $\mathbf{Q}(\sqrt{2})$ et donc $[\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}(\sqrt{2})] > 1$.

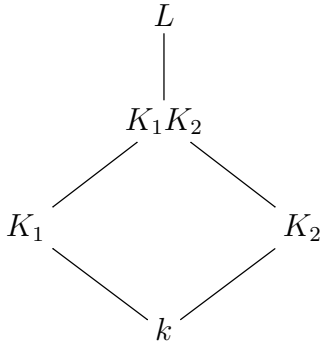
Notons ensuite que $\mathrm{Irr}(i, \mathbf{Q}) = X^2 + 1$, par conséquent $\mathrm{Irr}(i, \mathbf{Q}(\sqrt{2}))$ divise $X^2 + 1$ et ainsi $[\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}(\sqrt{2})] \leq 2$. Au total, $[\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}(\sqrt{2}] = 2$ et $[\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}] = [\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2} : \mathbf{Q}] = 4$. Au passage, on note que $(1, i)$ forme une $\mathbf{Q}(\sqrt{2})$-base de $\mathbf{Q}(i, \sqrt{2})$.

L'extension K/k est dite algébrique si **tous** les éléments de K sont algébriques sur k. Sinon, elle est dite transcendante. Toute extension K/k de degré fini est algébrique. Une extension de la forme $k(\alpha_1, \cdots, \alpha_n)/k$ est une extension algébrique si et seulement si tous les éléments α_i sont algébriques sur k. En fait Tout compositum d'extensions quelconques $K_i, i \in I$, de k (contenues dans K) est une extension algébrique de k si et seulement si toutes les extensions K_i/k, $i \in I$, sont algébriques. Les extensions L/K et K/k sont algébriques si et seulement L/k est algébrique.

(•) Extensions linéairement disjointes.

Rappelons le résultat suivant :

Proposition 3.3. *Soit L/k une extension algébrique et considérons des sous-extensions K_1/k et K_2/k de L/k :*



Alors toute famille d'éléments $(e_i)_{i \in I}$ de K_2 engendrant K_2 comme k-espace vectoriel, engendre K_1K_2 comme K_1-espace vectoriel. En particulier, si $[K_2 : k]$ est fini, $[K_1K_2 : K_1] \leq [K_2 : k]$.

On définit alors :

Définition 3.4. Soient des sous-extensions K_1/k et K_2/k de L/k. On dit que l'extension K_2 est linéairement disjointe de K_1 sur k si toute famille de K_2 libre sur k est libre sur K_1 (lorsque celle-

ci est vue dans le compositum K_1K_2). De manière équivalente : K_2 est linéairement disjointe de K_1 sur k si et seulement si toute k-base de K_2 est une K_1-base de K_1K_2.

Supposons l'extension K_2 de degré fini sur k, alors l'extension K_2 est linéairement disjointe de K_1 sur k si et seulement si $[K_1K_2 : K_1] = [K_2 : k]$. Plus généralement, l'extension K_2 est linéairement disjointe de K_1 sur k si et seulement si l'extension K_1 est linéairement disjointe de K_2 sur k. Si K_1/k et K_2/k sont toutes les deux finies et si les entiers $[K_1 : k]$ et $[K_2 : k]$ sont premiers entre eux, alors les extensions K_1/k et K_2/k sont linéairement disjointes.

Exemple 3.5. On peut montrer le résultat suivant (exercice) : si k un corps et $k(X)$ le corps des fractions rationnelles en une indéterminée alors toute extension algébrique K/k est linéairement disjointe de $k(X)/k$.

3.2 Clôture algébrique

(•) Corps de décomposition, corps de rupture.

Soit k un corps et P dans $k[X]$ non nul. Soit K/k une extension. Alors,

– on dit que K est un *corps de rupture* pour P s'il existe une racine α de P dans K telle que $K = k(\alpha)$,

– on dit que K est un *corps de décomposition* (ou *corps des racines* pour P si dans $K[X]$, le polynôme P se factorise en produit de polynômes de degré 1 et K est minimal pour cette propriété : $P = a_n \prod_{i=1}^{n}(X - \alpha_i)$, avec $\alpha_i \in K$ et $K = k(\alpha_1, \cdots, \alpha_n)$.

Exemple 3.6. On considère l'extension $\mathbf{C}/\mathbf{Q}$. Le corps des racines sur $\mathbf{Q}$ de $X^2 + 1$ est le corps $\mathbf{Q}(i)$. Le corps $\mathbf{Q}(\sqrt[3]{2})$ est un corps de rupture du polynôme $P = X^3 - 2$. On peut vérifier que le corps des racines sur $\mathbf{Q}$ de $X^3 - 2$ est le corps $\mathbf{Q}(\sqrt[3]{2}, j)$ avec j étant une racine primitive cubique de 1.

(•) Théorèmes d'existence et d'unicité.

Si P est irréductible dans $k[X]$, le quotient $k[X]/(P)$ est un corps donc une extension de k et par construction, c'est un corps de rupture pour P. On obtient :

Théorème 3.7. *Soit k un corps et soit $P \in k[X]$, non constant.*

(1) Il existe un corps de rupture K pour P. Si P est irréductible, tous les corps de rupture de P sont isomorphes (à $k[X]/(P)$).

(2) Si $P \in k[X]$ est non nul, il admet un corps de décomposition. De plus, si K et K' sont deux corps de décomposition pour P alors il existe un k-isomorphisme entre K et K'.

Le deuxième point du théorème s'obtient par induction sur le degré d de P en travaillant dans l'extension K/k donnée par le premier point.

Rappelons qu'un corps K est dit algébriquement clos si tout polynôme non constant $P \in K[X]$ admet une racine dans K.

Théorème 3.8 (Théorème de Steinitz)**.** *Soit k un corps. Alors il existe une extension algébrique $\overline{k}/k$, avec $\overline{k}$ algébriquement clos. Le corps $\overline{k}$ s'appelle une clôture algébrique de k.*

De plus, les clôtures algébriques de k sont toujours k-isomorphes deux à deux.

Démonstration. Dans ces notes, on démontre uniquement l'existence. On commence d'abord par vérifier qu'il existe une extension L_1 de k dans laquelle tout polynôme non constant de $k[X]$ admet une racine. Pour cela on introduit une indéterminée X_P associée à tout polynôme non constant P et on considère l'algèbre avec une infinité d'indéterminées $A = k[(X_P)_P]$. Soit I l'idéal de A engendré par tous les $P(X_P)$ pour P parcourant $k[X] \setminus k$.

On montre que I n'est pas l'algèbre A toute entière. On procède par l'absurde et on suppose en vue d'une contradiction que $1 \in I$. Dans ce cas il existe un nombre fini de polynômes $P_1, \cdots P_n$ non constants dans $k[X]$ et des coefficients $g_1, \cdots, g_n$ dans A tels que $1 = g_1 P_1(X_{P_1}) + \cdots + g_n P_n(X_{P_n})$. Les g_i sont dans A donc sont des polynômes en un nombre fini N d'indéterminées X_{P_i} avec $i = 1 \cdots N$ et on prend $N \geq n$ pour englober $X_{P_1}, \cdots, X_{P_n}$. Soit alors K une extension finie de k dans laquelle chaque P_i admette au moins une racine α_i pour $i \leq n$ (on peut prendre pour K le corps des racines de $\prod_{i=1}^n P_i(X) \in k[X]$). On pose ensuite $\alpha_j = 0$ pour $n+1 \leq j \leq N$. Alors en évaluant en $X_{P_i} = \alpha_i$ l'équation $1 = g_1 P_1(X_{P_1}) + \cdots + g_n P_n(X_{P_n})$ on obtient la contradiction $1 = 0$. Par l'absurde cela démontre $I \neq A$.

Maintenant que $I \neq A$ on sait par le lemme de Krull (en réalité ce lemme est équivalent à l'axiome du choix) qu'il existe un idéal M maximal de A tel que $I \subset M$. Ainsi dans l'anneau quotient $L_1 = A/M$ qui est un corps contenant k on voit que la classe de X_{P_i} est une racine du polynôme $P_i(X) \in L_1[X]$.

On itère ensuite par induction ce procédé pour construire une suite de corps $k = L_0 \subset L_1 \subset \cdots \subset L_j \subset \cdots$ telle que tout polynôme non constant dans L_j admette une racine dans L_{j+1}. Soit $L = \bigcup_{i \in \mathbf{N}} L_i$. Alors L est un corps algébriquement clos qui contient k parce que si $P \in L[X]$ est non constant il existe un étage j tel que $P \in L_j[X]$ et donc P admet une racine dans $L_{j+1} \subset L$. Pour conclure puisque $k \subset L$ et que L est algébriquement clos on considère le corps $\bar{k}$ dont les éléments sont les éléments de L algébriques sur k. Alors $\bar{k}$ est un corps et est algébriquement clos parce que tout élément de L algébrique sur $\bar{k}$ est aussi algébrique sur k. □

Le théorème ci-dessous nous dit qu'une clôture algébrique est unique à isomorphisme près. Un isomorphisme entre deux clôtures algébriques d'un corps k n'est cependant pas unique lui-même : c'est en fait déjà le cas si les deux clôtures algébriques sont supposées égales. Par

exemple $\mathrm{Aut}_{\mathbf{R}}(\mathbf{C}) = \{\mathrm{Id}, \text{conjugaison}\}$: il existe donc deux $\mathbf{R}$-isomorphismes différents entre $\mathbf{C}$ et $\mathbf{C}$ lui-même.

Exemple 3.9. Le corps $\mathbf{C}$ est une clôture algébrique de $\mathbf{R}$, mais pas de $\mathbf{Q}$. L'ensemble $\overline{\mathbf{Q}}$ des nombres complexes algébriques sur $\mathbf{Q}$ est une clôture algébrique de $\mathbf{Q}$. Elle est dénombrable : on peut écrire

$$\overline{\mathbf{Q}} = \bigcup_{P \in \mathbf{Q}[X]} \{ \text{ racines de } P \},$$

et on peut identifier $\mathbf{Q}[X]$ avec $\bigcup_{n \geq 1} \mathbf{Q}^n$ (en envoyant un polynôme P sur la suite de ses coefficients).

Proposition 3.10. *Soit K/k une extension algébrique. Alors le corps $\overline{k}$ est une clôture algébrique pour k si et seulement si $\overline{k}$ est une clôture algébrique pour K.*

3.3 Corps finis

(•) Construction des corps finis.

Soit k un corps fini, sa caractéristique est un nombre premier p, le sous-corps premier correspondant est $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. On obtient donc une extension nécessairement finie $k/\mathbf{F}_p$.

Le corps k est un $\mathbf{F}_p$-espace vectoriel de dimension finie $d \geq 1$. D'après la classification des espaces vectoriels, pour cette structure k est isomorphe à $\mathbf{F}_p^d$, donc de cardinal $|k| = p^d$.

Réciproquement, si $|k| = p^d$, alors k est une extension de degré d de $\mathbf{F}_p$.

Lemme 3.11. *Soit k un corps ayant p^d éléments. Alors pour tout $x \in k$, $x^{p^d} = x$.*

Démonstration. Soit $G = k^\times$ le groupe multiplicatif de k. Le groupe G est fini d'ordre $p^d - 1$ et, d'après le théorème de Lagrange, les éléments x non nul vérifient $x^{p^d - 1} = 1$.

En conclusion les éléments de k véifient $x^{p^d} = x$. □

Théorème 3.12. *Soit $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$. Pour tout entier d il existe une unique sous-extension de $\overline{\mathbf{F}}_p/\mathbf{F}_p$, de degré d, notée $\mathbf{F}_{p^d}$. L'extension $\mathbf{F}_{p^d}/\mathbf{F}_p$ est le corps des racines du polynôme $X^{p^d} - X$.*

Démonstration. D'après le lemme précédent il suffit de démontrer que le corps des racines de $X^{p^d} - X$ est de degré d sur $\mathbf{F}_p$. Cela revient à démontrer que l'ensemble des racines de $X^{p^d} - X$ dans $\overline{\mathbf{F}}_p$ est un sous-corps. La structure de sous-groupe additif est donnée par le petit théorème de Fermat, qui assure la $\mathbf{F}_p$-linéarité de l'application $t \mapsto t^p$ en caractéristique p. L'application $t \mapsto t^{p^d} - t$ est donc $\mathbf{F}_p$-linéaire, et l'ensemble des racines de $X^{p^d} - X$ est le noyau de cette

application. Les racines non nulles de $X^{p^d} - X$ forment un sous-groupe du groupe multiplicatif $\overline{\mathbf{F}}_p^\times$, donné par le noyau de l'élévation à la puissance $p^d - 1$. L'ensemble des racines de $X^{p^d} - X$ est donc bien un sous-corps de $\overline{\mathbf{F}}_p$. □

Exemple 3.13. Soit $k = \mathbf{F}_2$ et soit $P = X^2 + X + 1 \in k[X]$. Comme P n'a pas de racine dans k, le polynôme P est irréductible sur k. Soit θ une racine de P dans $\overline{k}$. Alors $[k(\theta) : k] = 2$, $|k(\theta)| = 2^2$ et donc $k(\theta) = \mathbf{F}_4$. On obtient aussi que tout élément x de $\mathbf{F}_4$ s'écrit de manière unique : $x = a + b\theta$, avec $a, b \in \{0, 1\}$.

Proposition 3.14. *Soient deux sous-extensions finies $k/\mathbf{F}_p$ et $k'/\mathbf{F}_p$ de $\overline{\mathbf{F}}_p/\mathbf{F}_p$. Si $|k| = p^d$ et $|k'| = p^{d'}$, alors $k \subset k'$ si et seulement si d divise d'.*

Démonstration. Supposons d'abord que d divise d', i.e. il existe n tel que $d' = nd$. Alors

$$p^{d'} - 1 = (p^d - 1)(p^{d(n-1)} + \cdots + p^d + 1)$$

et on voit que $p^d - 1$ divise $p^{d'} - 1$. En particulier, les racines de $X^{p^d} - X$ sont des racines de $X^{p^{d'}} - X$. On obtient $k \subset k'$. Réciproquement si $k \subset k'$ alors k' est un k-espace vectoriel de dimension finie notée n. On a donc $|k'| = |k|^n$ et $d' = nd$. □

Proposition 3.15. *Soit un corps fini k. Alors le groupe $k^\times$ est cyclique.*

Démonstration. Soit le groupe $G = (k^\times, \cdot)$, c'est un groupe commutatif, on peut donc introduire l'exposant e de $|k^\times| = p^d$. L'entier e est le ppcm des ordres des éléments de $|k^\times|$ et d'après le théorème de Lagrange, e divise $|k^\times|$. Puisque $k^\times$ est commutatif, il existe un élément α d'ordre e. Pour montrer que $k^\times$ est cyclique, il suffit donc de montrer que $e = p^d - 1$.

Le polynôme $X^e - 1$ admet pour dérivé $D(X^e - 1) = eX^{e-1}$, et $\operatorname{pgcd}(X^e - 1, eX^{e-1}) = 1$, donc $X^e - 1$ est séparable. Les éléments de $k^\times$ sont racines de ce polynôme (puisque tous les éléments de $|k^\times|$ sont d'ordre divisant e), et ils forment aussi l'ensemble des racines de $X^{p^d-1} - 1$. Ce dernier polynôme étant séparable, il divise donc $X^e - 1$, puis $p^d - 1$ est inférieur à e (en fait divise e), donc $e = p^d - 1$. Cela signifie que $k^\times$ est cyclique. □

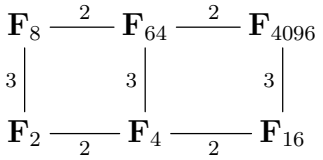
Proposition 3.16. *Soit $n = p^d m$ avec $\operatorname{pgcd}(m, p) = 1$ et soit k un corps fini de caractéristique p. Le sous-groupe des racines n-ièmes de l'unité de $\overline{k}^\times$ est d'ordre m. L'élévation à la puissance p est un isomorphisme de groupe de $\overline{k}^\times$ dans lui-même.*

Démonstration. On a un problème de séparabilité pour le polynôme $X^n - 1$ sur $\mathbf{F}_p$ lorsque p divise n. En effet si $\beta^p = \alpha$ dans $\overline{k}$, alors $X^p - \alpha = (X - \beta)^p$. D'où l'égalité $X^{p^d m} - 1 = (X^m - 1)^{p^d}$. Puis m étant premier avec p, le polynôme $X^m - 1$ est séparable et admet m racines distinctes dans $\overline{k}$. □

Corollaire 3.17. *Le treillis des sous-extensions de $\mathbf{F}_{p^n}$ correspond au treillis des diviseurs de n.*

Démonstration. Le résultat découle de la proposition 3.14. □

Exemple 3.18. Le corps $\mathbf{F}_{2^{12}}$ a pour sous-corps le treillis suivant :



(•) **Automorphismes.**

Si q est une puissance d'une nombre premier alors, à un isomorphisme de corps près, il y a un unique corps de cardinal q. Cette identification n'est cependant pas canonique, car plusieurs présentations (de $\mathbf{F}_q$) sont possibles :

Théorème 3.19. *Si $q = p^d$ alors les $\mathbf{F}_p$-automorphismes du corps $\mathbf{F}_q$ forment un groupe cyclique :*

$$\mathrm{Aut}_{\mathbf{F}_p}(\mathrm{F}_q) = \{1, \varphi, \varphi^2, \cdots, \varphi^{d-1}\}$$

de cardinal $d = [\mathbf{F}_q : \mathbf{F}_p]$ engendré par le morphisme de Frobenius :

$$\varphi : x \in \mathbf{F}_q \mapsto x^p \in \mathbf{F}_q.$$

Démonstration. Le morphisme de corps $\varphi : \mathbf{F}_q \to \mathbf{F}_q$ est un $\mathbf{F}_p$-morphisme (car il fixe le sous-corps $\mathbf{F}_p$ de $\mathbf{F}_q$ constitué des éléments x tels que $x^p = x$) dont les itérées $\varphi^k = \varphi \circ \varphi \circ \cdots \circ \varphi$ sont deux à deux distinctes jusqu'à l'ordre $d-1$. En effet, si $\varphi^k = \varphi^\ell$ avec $0 \leq k < \ell < d$ donnerait

$$\forall x \in \mathbf{F}_q, \quad x^{p^{\ell-k}} = x \text{ avec } 0 < \ell - k < d,$$

d'où un polynôme de degré $p^{\ell-k} < p^d = q$ avec q racines, ce qui est absurde. Par ailleurs, un $\mathbf{F}_p$-morphisme du corps $\mathbf{F}_q$ étant complètement déterminé par l'image d'un générateur de $\mathbf{F}_q$, il y a au plus $\dim_{\mathbf{F}_p}(\mathbf{F}_q) = [\mathbf{F}_q : \mathbf{F}_p]$ tels morphismes. Finalement on obtient que l'inclusion $\mathrm{Aut}_{\mathbf{F}_p}(\mathrm{F}_q) \subset \{1, \varphi, \varphi^2, \cdots, \varphi^{d-1}\}$ avec $d = [\mathbf{F}_q : \mathbf{F}_p]$ est une égalité en utilisant l'inégalité

$$|\mathrm{Aut}_{\mathbf{F}_p}(\mathrm{F}_q)| \leq [\mathbf{F}_q : \mathbf{F}_p].$$

□

(•) **Clôture algébrique des corps finis.**

Soit $\mathbf{F}_q$ avec $q = p^d$ un corps fini. On peut décrire la clôture algébrique $\overline{\mathbf{F}}_q$ de la manière suivante :

$$\overline{\mathbf{F}}_q = \overline{\mathbf{F}}_p = \bigcup_{n \in \mathrm{N}^*} \mathbf{F}_{p^n}.$$

Justifions cette description. Puisque $\mathbf{F}_q$ est algébrique sur $\mathbf{F}_p$, leurs clôtures algébriques sont égales. Commençons par donner un sens à l'union $\bigcup_{n\in\mathbb{N}^*} \mathbf{F}_{p^n}$. On sait que la clôture algébrique $\overline{\mathbf{F}}_p$ existe et que chaque corps $\mathbf{F}_{p^n}$ est contenu dans (par exemple) $\mathbf{F}_{p^{n!}}$ qui lui-même est contenu dans $\overline{\mathbf{F}}_p$. De plus on a des inclusions $\mathbf{F}_{p^{n!}} \subset \mathbf{F}_{p^{(n+1)!}}$. Ainsi l'union $U := \bigcup_{n\in N^*} \mathbf{F}_{p^n} = \bigcup_{n\in N^*} \mathbf{F}_{p^{n!}}$ est bien un sous-corps de $\overline{\mathbf{F}}_p$. De plus, U est algébriquement clos : si P est un polynôme de $U[X]$ alors il existe m suffisamment grand tel que P est dans $\mathbf{F}_{p^m}[X]$. Les racines de P appartiennent alors au corps de décomposition de P qui est lui-même égal à un corps $\mathbf{F}_{p^n}$ avec $n \geq m$. Donc les racines de P sont toutes dans U et U est bien algébriquement clos. Finalement, puisque U est de caractéristique p, il contient $\mathbf{F}_p$ et il est contenu dans tout corps algébriquement clos de caractéristique p (car un tel corps contient, pour tout n, les solutions de $x^{p^n} - x = 0$ donc $\mathbf{F}_{p^n}$). On obtient finalement que U est la clôture algébrique de $\mathbf{F}_p$, comme annoncé.

4 Polynômes

Tous les anneaux considérés seront commutatifs. On désigne toujours par A un anneau commutatif et K un corps.

4.1 Propriété universelle des algèbres de polynômes

Théorème 4.1. *Soit A un anneau commutatif et B une A-algèbre. Soit $n \geq 1$ un entier. Soient $\mathbf{b} := (b_1, \ldots, b_n)$ un n-uplet d'éléments de B qui commutent deux à deux. Alors il existe un unique morphisme de A-algèbres $\varphi_{\mathbf{b}} = \mathrm{ev}_{\mathbf{b}} : A[X1, ..., Xn] \to B$ tel que $\varphi_{\mathbf{b}}(X_i) = b_i$ pour tout i dans $[|1, n|]$.*

En particulier, on en déduit :

Corollaire 4.2. *(1) On a un isomorphisme d'algèbres naturel*

$$A[X_1, \ldots, X_n][X_{n+1}] \simeq A[X_1, \ldots, X_n, X_{n+1}].$$

(2) À tout polynôme P de $A[X_1, \ldots, Xn]$, est associée une fonction polynômiale

$$f_P : A^n \to A \quad \textit{donnée par} \quad (a_0, \ldots, a_n) \mapsto P(a_0, \ldots, a_n).$$

4.2 Polynômes irréductibles

Dans cette partie A est un anneau intègre et on note $K := \mathrm{Frac}(A)$.

(•) Le cas où A est factoriel.

On va montrer que si A est factoriel alors $A[X]$ est aussi factoriel. Pour cela, on introduit la définition suivante :

Définition 4.3. Soient A un anneau factoriel et $P := \sum_{n=0}^{d} a_n X^n$ un polynôme non nul de $A[X]$. Le contenu de P, noté $c(P)$, est défini comme le pgcd des a_n pour $0 \leq n \leq d$. On dit que P est primitif si $c(P) = 1$.

Le contenu satisfait les propriétés suivantes :

Proposition 4.4. *Soit A un anneau factoriel de corps de fraction K.*

(1) Soit P un polynôme non nul de $A[X]$. Il existe un unique polynôme primitif $\widetilde{P}$ de $A[X]$ tel $P = c(P)\widetilde{P}$.

(2) Si P et Q sont deux polynômes non nuls de $A[X]$, on a $c(PQ) = c(P)c(Q)$.

(3) Si P est un polynôme non nul de $K[X]$ alors il existe α dans $K^\times$ et $\widetilde{P}$ dans $A[X]$ primitif tel que $P = \alpha\widetilde{P}$. La paire $(\alpha, \widetilde{P})$ est unique à une unité de A près.

Démonstration. (1) Écrivons $P := \sum_{i=0}^{d} a_i X^i$. Pour tout i entre 0 et d, on peut écrire $a_i = c(P)\widetilde{a}_i$ avec $\widetilde{a}_i$ dans A. On pose $\widetilde{P} := \sum_{i=0}^{d} \widetilde{a}_i X^i$. On a bien $P = c(P)\widetilde{P}$. De plus, si p est un irréductible de A, on a

$$v_p(c(P)) = \min\{v_p(a_i), 0 \leq i \leq d\} = v_p(c(P)) + \min\{v_p(\widetilde{a}_i), 0 \leq i \leq d\} = v_p(c(P)) + v_p(c(\widetilde{P})),$$

et donc $v_p(c(\widetilde{P})) = 0$. D'où $c(\widetilde{P}) = 1$.

(2) Remarquons d'abord que si $\alpha \in A$, alors $c(\alpha P) = \alpha c(P)$. Puisque, par (1), tout polynôme non nul P s'écrit $P = c(P)\widetilde{P}$ avec $c(\widetilde{P}) = 1$, il suffit de montrer que si $c(P) = c(Q) = 1$ alors $c(PQ) = 1$. En effet, si $P = c(P)\widetilde{P}$ et $Q = c(Q)\widetilde{Q}$, on a $PQ = c(P)c(Q)\widetilde{P}\widetilde{Q}$ et $c(PQ) = c(P)c(Q)c(\widetilde{P}\widetilde{Q})$.

Plaçons nous alors dans ce cas. Supposons par l'absurde qu'il existe un irréductible p de A divisant $c(PQ)$. Considérons l'anneau intègre $(A/p)[X]$. Puisque $c(P) = c(Q) = 1$, les images $\overline{P}$ et $\overline{Q}$ de P et Q sont non nulles (sinon p diviserait $c(P)$ et $c(Q)$). Mais on a $\overline{PQ} = 0$ avec $\overline{P}$ et $\overline{Q}$ non nuls, ce qui est impossible.

(3) **Existence :** Soit a dans A tel que aP dans $A[X]$. Alors par (1), on a $aP = c(aP)\widetilde{P}$ avec $a \neq 0$ dans K et Q primitif de $A[X]$. Alors la paire $(\alpha, \widetilde{P})$ avec $\alpha = \frac{c(aP)}{a}$ convient.

Unicité : Supposons que $P = \alpha Q = \beta R$ avec Q et R dans $A[X]$ primitifs. On choisit a un élément non nul de A tel que $a\alpha$ et $a\beta$ sont dans A. Alors $c(aP) = c(a\alpha) = c(a\beta)$. En d'autres termes, il existe une unité u dans $A^\times$ tel que $a\beta = ua\alpha$. Puisque a est intègre, on obtient $\beta = u\alpha$, comme voulu. □

On peut maintenant déterminer les éléments irréductibles de $A[X]$.

Proposition 4.5. *Soit A un anneau factoriel. Alors les polynômes irréductibles sur A sont exactement les constantes irréductibles dans A et les polynômes primitifs non constants irréductibles dans $K[X]$.*

Remarque 4.6. Il faut cependant faire attention que si A est factoriel avec $K = \mathrm{Frac}(A)$ et P est un polynôme de $A[X]$ qui est irréductible dans $K[X]$ alors P n'est pas nécessairement irréductible dans $A[X]$. Considérons par exemple le polynôme $P = 2X$ dans $\mathbf{Z}[X]$: il n'est pas irréductible dans $\mathbf{Z}[X]$ (puisque produit de 2 et de X, aucun n'étant inversible) mais il le devient dans $\mathbf{Q}[X]$ (puisque 2 est alors inversible).

Démonstration. Si $P = a$ est constant et $P = QR$ avec Q et R dans $A[X]$, on a $\deg(Q) + \deg(R) \leq 0$, donc Q et R sont constants. Comme on a aussi $A[X]^\times = A^\times$, on en déduit que a est irréductible dans A si et seulement si, il l'est dans $A[X]$.

Supposons maintenant que le degré de P est > 0. On veut montrer que P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $K[X]$ et $c(P) = 1$.

Montrons l'implication dans le sens direct. Si P est irréductible dans $A[X]$, puisque $P = c(P)\widetilde{P}$ avec $\widetilde{P}$ non inversible dans $A[X]$ (sinon il serait constant et P lui-même serait constant), on a nécessairement $c(P) = 1$. Si $P = QR$ avec Q et R dans $K[X]$, en écrivant (par Proposition 4.4(3)) $Q = \alpha\widetilde{Q}$ et $R = \beta\widetilde{R}$ avec α, β dans K et $\widetilde{Q}, \widetilde{R}$ dans $A[X]$ primitifs. Alors, puisque $P = \alpha\beta\widetilde{Q}\widetilde{R}$ est dans $K[X]$, par l'unicité dans Proposition 4.4(3), on a $\alpha\beta$ inversible dans A. On obtient que soit $\widetilde{Q}$ soit $\widetilde{R}$ est dans $A^\times$ par irréductibilité de P dans $A[X]$. Ainsi soit Q soit R est dans $K^\times$. On obtient donc bien que P est irréductible dans $K[X]$.

Réciproquement, si P est irréductible dans $K[X]$ et si $P = QR$, on obtient $Q \in A \cap K^\times = A \setminus \{0\}$ ou $R \in A \cap K^\times$. On a de plus $c(P) = 1 = c(Q)c(R)$ et comme $Q = c(Q)$ et $R = c(R)$, on obtient bien que Q ou R est une unité de A. □

On peut maintenant montrer le résultat principal de cette section :

Théorème 4.7. *Si A est un anneau factoriel alors $A[X]$ est factoriel. Par récurrence, pour tout n, l'anneau $A[X_1, \ldots, X_n]$ est lui aussi factoriel.*

Démonstration. **Existence.** Soit $P \in A[X] \subset K[X]$, non nul. L'anneau $K[X]$ est principal (il est même euclidien) donc factoriel, et il existe donc des irréductibles $Q_1, \ldots, Q_r$ de $K[X]$ et v dans $K[X]^\times = K^\times$ tels que

$$P = vQ_1^{m_1} \ldots Q_r^{m_r}.$$

Pour chaque i, il existe α_i dans $K^\times$ et $\widetilde{Q}_i$ primitif dans $A[X]$ tel que $Q_i = \alpha_i\widetilde{Q}_i$. Puisque Q_i est irréductible dans $K[X]$, on a que $\widetilde{Q}_i$ est irréductible dans $K[X]$ et comme il est primitif, le résultat précédent nous donne qu'il est irréductible dans $A[X]$. On note

$$u := v\prod_{i=1}^{r}\alpha_i \in K^\times \quad \text{et} \quad Q = \prod_{i=1}^{r}\widetilde{Q}_i^{m_i} \text{ primitif dans } A[X].$$

On obtient $P = uQ$ et $P = c(P)\widetilde{P}$. Par unicité, il existe une unité λ de A telle que $u = \lambda c(P)$. Il suit que u est dans $A \setminus \{0\}$ et puisque A est factoriel, on peut écrire u comme un produit d'irréductibles de A, donc de $A[X]$. On obtient bien que P lui-même est un produit d'irréductibles de $A[X]$.

Unicité. Supposons que

$$P = u\prod_{j\in J} q_j^{n_j}\prod_{i\in I} P_i^{m_i} = v\prod_{j\in J} q_j^{n'_j}\prod_{i\in I} P_i^{m'_i},$$

avec $u, v \in A^\times$, q_j irréductibles de A (donc de $A[X]$) et P_i polynômes primitifs de $A[X]$ irréductibles dans $K[X]$. Puisque $K[X]$ est factoriel, l'unicité de la décomposition dans $K[X]$ implique

que $m_i' = m_i$. Puisque $A[X]$ est intègre, on a ensuite l'égalité

$$u \prod_{j \in J} q_j^{n_j} = v \prod_{j \in J} q_j^{n_j'}$$

dans A. Puisque A est factoriel, on obtient finalement $n_j = n_j'$ pour tout j de J.

□

(•) Exemples de polynômes irréductibles.

On rappelle que si K est un corps, l'anneau $K[X]$ est principal. Ainsi, pour P est un polynôme non nul sur K, on voit que P est irréductible si et seulement si (P) est un idéal premier de $K[X]$, si et seulement si (P) est un idéal maximal de $K[X]$, si et seulement si $K[X]/(P)$ est un corps. De plus, si P est de degré inférieur ou égal à 3, on vérifie que P est irréductible sur K si et seulement si P n'admet aucune racine dans K. Par conséquent, si K est algébriquement clos, les irréductibles de $K[X]$ sont exactement les polynômes de degré 1.

Si A est un anneau factoriel, on a vu plus haut que P dans $A[X]$ est irréductible si et seulement si P est irréductible dans $K[X]$ et P est primitif. On peut utiliser les critères suivants :

Proposition 4.8 (Critère d'Eisenstein)**.** *Soit A un anneau factoriel. Soit $P(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme à coefficients dans A de contenu 1. On suppose l'existence d'un idéal premier $\mathfrak{p}$ de A tel que*

- *les coefficients $a_0, \cdots, a_{n-1}$ appartiennent à $\mathfrak{p}$,*
- *le coefficient dominant a_n n'appartient pas à $\mathfrak{p}$,*
- *le coefficient constant a_0 n'appartient pas au produit $\mathfrak{p}^2$.*

Alors le polynôme P est irréductible sur le corps de fractions K de A.

Exemple 4.9. (1) Le polynôme $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$ est irréductible sur $\mathbf{Q}$ (où p est un nombre premier). En effet, si on considère l'automorphisme de $\mathbf{Z}[X]$ qui envoie un polynôme P sur le polynôme $P(X+1)$, on voit qu'il suffit de montrer que $\Phi_p(X+1)$ est irréductible. Or, en réduisant modulo p, on obtient

$$X\Phi_p(X+1) = X^p \bmod p \text{ dans } \mathbf{F}_p[X]$$

et puisque $\mathbf{F}_p[X]$ est intègre, on en déduit :

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

Les coefficients de $\Phi_p(X+1)$ sont donc tous divisibles par p, à l'exception du coefficient dominant. On a de plus $\Phi_p(1) = p$ donc p^2 ne divise pas le coefficient constant de $\Phi_p(X+1)$. On applique le critère d'Eisenstein : $\Phi_p(X+1)$ (et donc $\Phi_p(X)$) est bien irréductible sur $\mathbf{Q}$.

(2) En appliquant le critère d'Eisenstein pour n'importe quel premier de $\mathbf{Z}$, on voit que les polynômes $X^n - a$ sont irréductibles sur $\mathbf{Q}$ pour tout $a \neq 1$ sans facteur carré.

Proposition 4.10. *Soient A un anneau factoriel et K son corps de fraction. Soit P dans $A[X]$, on note a_d son coefficient dominant. Soit I un idéal premier de A et $L = \mathrm{Frac}(A/I)$. Alors, si a_d n'est pas dans I et la réduction $\overline{P}$ de P dans $L[X]$ est un polynôme irréductible, P lui-même est irréductible dans $K[X]$.*

4.3 Polynômes à plusieurs variables

(•) Polynômes homogènes.

On rappelle qu'un polynôme de $A[X_1, \ldots, X_n]$ est dit homogène de degré d si les monômes non nuls qui le constituent sont tous de degré (total) d, i.e. on peut écrire

$$P = \sum_{\sum_{i=1}^n m_i = d} a_{(m_1,\ldots,m_n)} X_1^{m_1} \cdots X_n^{m_n}.$$

Par exemple, le déterminant

$$\det = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^n X_{\sigma(j),j}$$

est un polynôme homogène de degré n, à n^2 variables.

L'ensemble des polynômes homogènes de degré d forme un A-module libre de base $(X_1^{\alpha_1} \cdots X_n^{\alpha_n})_{\alpha \text{ t.q. } \sum_{i=1}^n \alpha_i = d}$. En particulier, on voit qu'il est de rang $\binom{n+d-1}{d}$ (nombre de combinaisons avec remise de d éléments parmi n : la valeur de α_i correspond au nombre de fois où on a choisi l'objet i). On a :

Proposition 4.11. *Soit P dans $A[X_1, \ldots, X_n]$ et on considère le polynôme de $A[X_1, \ldots, X_n][T]$ donné par $Q(T) := P(TX_1, \ldots, TX_n)$. Les assertions suivantes sont équivalentes :*

(1) le polynôme P de $A[X_1, \ldots, X_n]$ est homogène de degré d,

(2) on a $Q(T) = T^d P(X_1, \ldots, X_n)$,

(3) le polynôme $Q(T)$ est un monôme de degré d.

En conséquence, on obtient que tout P de $A[X_1, \ldots, X_n]$ s'écrit de manière unique sous la forme

$$P = \sum_{d \geq 0} P_d,$$

où P_d est un polynôme homogène de degré d de $A[X_1, \ldots, X_n]$.

Démonstration. Clair en écrivant

$$P = \sum_{(m_1,\ldots m_n)} a_{(m,1,\ldots,m_n)} X_1^{m_1} \cdots X_n^{m_n} \quad \text{et} \quad Q(T) = \sum_{d \geq 0} \sum_{\sum_{i=1}^n m_i = d} a_{(m_1,\ldots,m_n)} X_1^{m_1} \cdots X_n^{m_n} T^d.$$

□

(•) **Polynômes symétriques.**

Un polynôme P de $A[X_1, \ldots, X_n]$ est dit symétrique si pour tout σ dans $\mathfrak{S}_n$ on a $\sigma \cdot P = P$. L'ensemble des polynômes symétriques en n variables est noté $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$. On vérifie que c'est une sous-A-algèbre de $A[X_1, \ldots, X_n]$.

Exemple 4.12. Le polynôme $X_1 + X_2$ est dans $A[X_1, X_2]^{\mathfrak{S}_2}$ mais si $n \geq 3$, le polynôme $X_1 + X_2$ n'est pas dans $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$. En particulier, le fait d'être symétrique dépend du nombre de variables considérées.

Définition 4.13 (Polynômes symétriques élémentaires)**.** Pour tout k dans N, on définit le k-ième polynôme symétrique (en n variables) par :

$$\sigma_k(X_1, \ldots, X_n) = \sum_{\substack{I \subseteq [|1;n|] \\ |I|=k}} \prod_{i \in I} X_i = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}.$$

On vérifie que pour tout k dans $[|1; n|]$, le polynôme $\sigma_k(X_1, \ldots, X_n)$ est homogène de degré k et symétrique. Son degré partiel en chaque variable est 1.

Exemple 4.14. (•) Si $n = 2$, on a

$$\begin{aligned} \sigma_1(X_1, X_2) &= X_1 + X_2 \\ \sigma_2(X_1, X_2) &= X_1 X_2 \end{aligned}$$

(•) Si $n = 3$, on a

$$\begin{aligned} \sigma_1(X_1, X_2, X_3) &= X_1 + X_2 + X_3 \\ \sigma_2(X_1, X_2, X_3) &= X_1 X_2 + X_2 X_3 + X_3 X_1 \\ \sigma_3(X_1, X_2, X_3) &= X_1 X_2 X_3 \end{aligned}$$

Théorème 4.15 (Relations coefficients-racines)**.** *On a dans l'anneau $A[X_1, \ldots, X_n, T]$:*

$$\prod_{i=1}^{n} (T - X_i) = \sum_{k=0}^{n} (-1)^{n-k} \sigma_{n-k}(X_1, \ldots, X_n) T^k.$$

En particulier,

Corollaire 4.16. *Soit $P(T) = \sum_{k=0}^{n} a_k T^k$ dans $A[T]$ de degré n et soient $\alpha_1, \ldots, \alpha_n$ ses racines dans $\overline{K}$ (où $K := \mathrm{Frac}(A)$) comptées avec multiplicité. Pour tout k entre 0 et n, on a :*

$$a_k = a_n (-1)^{n-k} \sigma_{n-k}(\alpha_1, \ldots, \alpha_n).$$

On rappelle aussi le théorème suivant, qui dit que tout polynôme symétrique en n variables s'écrit de manière unique comme un polynôme en les polynômes symétriques élémentaires en n variables :

Théorème 4.17 (Structure des polynômes symétriques)**.** *L'application*

$$\begin{array}{ccc} A[T_1,\dots,T_n] & \longrightarrow & A[X_1,\dots,X_n]^{\mathfrak{S}_n} \\ F(T_1,\dots T_n) & \longmapsto & F\left(\sigma_1(\underline{X}),\dots,\sigma_n(\underline{X})\right). \end{array}$$

est un isomorphisme de A-algèbres.

Exemple 4.18. On verra en TD un algorithme qui, pour un polynôme symétrique donné, permet d'obtenir son image par l'isomorphisme ci-dessus. Par exemple, an a la formule

$$\begin{aligned} X_1X_2^2+X_1X_3^2+X_2X_1^2+X_3X_1^2+X_2X_3^2+X_3X_2^2 &= \sigma_1(X_1,X_2,X_3)\sigma_2(X_1,X_2,X_3)-3\sigma_3(X_1,X_2,X_3) \\ &= F(\sigma_1(X_1,X_2,X_3),\sigma_2(X_1,X_2,X_3),\sigma_3(X_1,X_2,X_3)), \end{aligned}$$

où $F(T_1,T_2,T_3)=T_1T_2-3T_3$,

4.4 Polynômes cyclotomiques

(•) Définition et construction.

Cette construction des polynômes cyclotomiques ne dépend pas du corps de base :

Théorème 4.19. *Soit K un corps. Il existe une unique suite $(\Phi_{n,K})_n$ de polynômes unitaires de $K[X]$ telle que pour tout n de $\mathrm{N}_{\geq 1}$,*

$$X^n-1=\prod_{d|n}\Phi_{d,K}$$

dans $K[X]$.

Si $\iota : \mathbf{Z} \to K$ désigne le morphisme canonique qui envoie $1 \in \mathbf{Z}$ sur $1 \in K$ alors $\Phi_{n,K}=\iota(\Phi_{n,\mathbf{Q}})$. Cette propriété permet d'oublier le corps en notant simplement $\Phi_n := \Phi_{n,\mathbf{Q}}$ le n-ième polynôme éventuellement plongé dans $K[X]$ à travers ι.

Exemple 4.20. On a donc

$$X-1=\Phi_1,\quad X^2-1=\Phi_1\Phi_2,\quad X^3-1=\Phi_1\Phi_3,\quad X^4-1=\Phi_1\Phi_2\Phi_4,$$

et on en déduit :

$$\Phi_1=X-1,\quad \Phi_2=X+1,\quad \Phi_3=X^2+X+1,\quad \Phi_4=X^2+1.$$

Si on fixe le corps K, on obtient la définition suivante :

$$\Phi_{n,K} := \prod_{\zeta \text{ primitive}} (X - \zeta),$$

où le produit est pris sur l'ensemble des $\varphi(n)$ racines primitives de l'unité. En particulier, on voit que $\Phi_{n,K}$ est de degré $\varphi(n)$ où φ est la fonction indicatrice d'Euler.

(•) **Propriétés calculatoires.**

Proposition 4.21. *Pour tout $n \geq 2$, on a $\Phi_n = X^{\varphi(n)}\Phi_n\left(\frac{1}{X}\right)$. De plus, si p est un nombre premier alors,*

$$\begin{cases} \Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1, \\ \Phi_{p^\alpha} = \Phi_p \circ X^{p^{\alpha-1}}, \end{cases} \quad \begin{cases} \Phi_{pn} = \Phi_n \circ X^p, & \text{si } p \text{ divise } n, \\ \Phi_{pn}\Phi_n = \Phi_n \circ X^p, & \text{si } p \text{ ne divise pas } n. \end{cases}$$

Si $p_1, \ldots, p_m$ sont premiers distincts,

$$\Phi_{p_1^{\alpha_1} \cdots p_m^{\alpha_m}} = \Phi_{p_1 \cdots p_m} \circ X^{p_1^{\alpha_1 - 1} \cdots p_m^{\alpha_m - 1}}.$$

Démonstration. Exercice. □

(•) **Irréductibilité.**

On commencer par montrer le lemme suivant :

Lemme 4.22. *Soit P est un polynôme unitaire de $\mathbf{Z}[X]$. S'il existe Q dans $\mathbf{Q}[X]$ unitaire et R dans $\mathbf{Q}[X]$ tels que $P = QR$ alors Q est en fait dans $\mathbf{Z}[X]$.*

Démonstration. On utilise en fait le point (3) de la proposition 4.4, rappelons rapidement la construction. Il existe a non nul dans $\mathbf{Z}$ tel que aQ est dans $\mathbf{Z}[X]$ et b non nul dans $\mathbf{Z}$ tel que bR est dans $\mathbf{Z}[X]$. On pose $\alpha := \frac{c(aQ)}{a}$ et $\beta := \frac{c(bR)}{b}$ et comme le contenu de P est égal à 1, la décomposition $abP = (aQ)(bR)$ donne (en passant au contenu) $\alpha\beta = 1$. On peut écrire $Q = \alpha\widetilde{Q}$ et $R = \beta\widetilde{R}$ avec $\widetilde{Q}$ et $\widetilde{R}$ des polynômes primitifs de $\mathbf{Z}[X]$. On obtient donc

$$P = \alpha\beta\widetilde{Q}\widetilde{R} = \widetilde{Q}\widetilde{R} \text{ dans } \mathbf{Z}[X].$$

On en déduit que $\widetilde{Q}$ et $\widetilde{R}$ sont des polynômes unitaires de $\mathbf{Z}[X]$. Mais on a $Q = \alpha\widetilde{Q}$ avec Q et $\widetilde{Q}$ tous les deux unitaires. Donc $\alpha = 1$ et on obtient $Q = \widetilde{Q}$, ce qui montre que Q est bien dans $\mathbf{Z}[X]$. □

Théorème 4.23. *Le polynôme Φ_n est dans $\mathbf{Z}[X]$ et est irréductible dans $\mathbf{Z}[X]$ (et dans $\mathbf{Q}[X]$) pour tout $n \geq 1$. En d'autres termes, Φ_n est le polynôme minimal sur $\mathbf{Q}$ d'une/de toute racine n-primitive (complexe).*

Démonstration. On a vu qu'un polynôme unitaire de $\mathbf{Z}[X]$ est irréductible dans $\mathbf{Z}[X]$ si et seulement si il l'est dans $\mathbf{Q}[X]$.

On considère P dans $\mathbf{Q}[X]$ le polynôme minimal d'une racine primitive n-ième de l'unité $\zeta \in \mathbf{C}$. Par le lemme ci-dessus, comme P est unitaire et divise $X^n - 1$ un polynôme unitaire de $\mathbf{Z}[X]$, on voit que P est en fait dans $\mathbf{Z}[X]$. Pour prouver le théorème, il suffit donc de montrer que P est égal à Φ_n. Pour cela, on va montrer que pour tout premiers $p_1, \ldots, p_r$ qui ne divisent pas n, alors P est le polynôme minimal de la racine primitive n-ième $\zeta^{p_1^{\alpha_1} \cdots p_m^{\alpha_m}}$.

On considère p un nombre premier qui ne divise pas n. Soit Q dans $\mathbf{Q}[X]$ le polynôme minimal de la racine ζ^p (qui est elle-même une racine primitive n-ième de l'unité puisque $\mathrm{pgcd}(n, p) = 1$). Par le lemme, on a encore que Q est dans $\mathbf{Z}[X]$. On veut montrer que $P = Q$. On suppose $P \neq Q$. Dans ce cas, puisque P et Q divisent Φ_n, le produit PQ divise aussi Φ_n dans $\mathbf{Q}[X]$. Puisque PQ est unitaire, on voit qu'en fait PQ divise Φ_n dans $\mathbf{Z}[X]$. En réduisant modulo p, on obtient que $\overline{PQ}$ divise $\overline{\Phi}_n = \Phi_{n,\mathbf{F}_p}$ dans $\mathbf{F}_p[X]$. De plus, puisque $(Q \circ X^p)(\zeta) = 0$ et que P est minimal, on voit que P divise $Q \circ X^p$ dans $\mathbf{Q}[X]$ donc dans $\mathbf{Z}[X]$ (puisque $Q \circ X^p$ et P sont unitaires). Ainsi, en réduisant modulo p, on obtient que $\overline{P}$ divise $\overline{Q \circ X^p} = (\overline{Q \circ X})^p = (\overline{Q})^p$ dans $\mathbf{F}_p[X]$. Si π est un irréductible de $\mathbf{F}_p[X]$, on a alors que si π divise $\overline{P}$, il divise aussi $\overline{Q}$ et donc π^2 divise $\overline{PQ}$ qui lui-même divise $\overline{\Phi}_n$ et donc $X^n - 1$. Mais si p et n sont premiers entre eux alors $X^n - 1$ est séparable dans $\mathbf{F}_p[X]$, ce qui donne une contradiction. On a donc $P = Q$ et P est bien le polynôme minimal à la fois de ζ et ζ^p.

En répétant l'argument, on obtient ensuite que P est le polynôme minimal de la racine primitive n-ième $\zeta^{p_1^{\alpha_1} \cdots p_m^{\alpha_m}}$ pour tout premiers $p_1, \ldots p_r$ et donc de toute racine primitive n-ième de l'unité. Finalement, on a montré que Φ_n n'a qu'un seul facteur irréductible P : il est donc lui-même irréductible dans $\mathbf{Q}[X]$. □

En TD, on prouvera :

Théorème 4.24. *Le polynôme cyclotomique Φ_n est irréductible dans $\mathbf{F}_q[X]$ si et seulement si l'entier q est générateur du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$.*

On termine cette section par la caractérisation suivante (appelée parfois "caractérisation de Kronecker") :

Théorème 4.25. *Soit P un polynôme de $\mathbf{Q}[X]$. Alors P est un polynôme cyclotomique (i.e. il existe $n \geq 1$ tel que $P = \Phi_n$) si et seulement si P est dans $\mathbf{Z}[X]$, qu'il est unitaire et irréductible, et à racines complexes toutes non nulles de module ≤ 1.*

Démonstration. Le sens direct est clair. Supposons alors que P est un polynôme unitaire de $\mathbf{Z}[X]$, irréductible et dont les racines $x_i, 1 \leq i \leq n$, sont non nulles et dans $\mathbf{D} := \{z \in \mathbf{C} \mid |z| \leq 1\}$. On considère le polynôme symétrique en $(x_1, \ldots, x_n)$:

$$P_j(x_1, \ldots, x_n) := \prod_{1 \leq i \leq n} (X - x_i^j).$$

Alors $P_j(x_1, \ldots, x_n)$ est en fait dans $\mathbf{Z}[X]$: comme $P_j(x_1, \ldots, x_n)$ est symétrique en $(x_1, \ldots, x_n)$, il s'écrit sous la forme $Q_j(\sigma_1, \ldots, \sigma_n)$ avec $Q_j \in \mathbf{Z}[X][T_1, \ldots, T_n]$, où les σ_i sont les polynômes symétriques élémentaires en $(x_1, \ldots, x_n)$. Par les relations coefficients-racines, les σ_i sont les coefficients de P et ils appartiennent donc bien à $\mathbf{Z}$. Ainsi $P_j(x_1, \ldots, x_n)$ est bien dans $\mathbf{Z}[X]$.

On peut de plus écrire

$$P_j(x_1, \ldots, x_n) = X^n + \sum_{1 \leq k \leq n} (-1)^k \sigma_k(x_1^j, \ldots, x_n^j) X^{n-k}$$

(et on a donc montré ci-dessus que $\sigma_k(x_1^j, \ldots, x_n^j) \in \mathbf{Z}$). Comme les x_i sont dans $\mathbf{D}$ on a

$$|\sigma_k(x_1^j, \ldots, x_n^j)| = |\sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1}^j \cdots x_{i_k}^j| \leq \sum_{1 \leq i_1 < \cdots < i_k \leq n} 1 = \binom{n}{k},$$

ce qui montre que les $\sigma_k(x_1^j, \ldots, x_n^j)$ ne peuvent prendre qu'un nombre fini de valeurs quand j varie. Ainsi la famille $\{P_j(x_1, \ldots, x_n)\}_{j \in \mathrm{N}}$ est finie, et en particulier, l'ensemble des racines $\{x_i^j\}_{1 \leq i \leq n \text{ et } j \in \mathrm{N}}$ est lui aussi fini. Comme pour un i fixé, il suit que $\{x_i^j\}_{j \in \mathrm{N}}$ est lui-même fini, on obtient qu'il existe $j_1 \neq j_2$ tel que $x_i^{j_1} = x_i^{j_2}$: ainsi soit $x_i = 0$, soit x_i est une racine de l'unité.

Soit m l'ordre d'une des racines x_i. Puisque P est le polynôme minimal sur $\mathbf{Q}$ de x_i, il divise $X^m - 1$. Les polynômes cyclotomiques étant les facteurs irréductibles de $X^m - 1$, il s'ensuit qu'il existe d un diviseur de m tel que $P = \Phi_d$. Ceci termine la preuve du théorème. □

5 Formes quadratiques

Dans cette section on suppose que K est un corps de caractéristique différente de 2.

5.1 Définitions

Soit V un K-espace vectoriel de dimension finie. Une forme quadratique q sur V est une application $q : V \to K$ telle qu'il existe $b_q : V \times V \to K$ une forme bilinéaire symétrique vérifiant, pour tout x de V, $q(x) = b_q(x, x)$. La forme b_q est alors uniquement déterminée par les formules

$$b_q(x, y) = \frac{q(x+y) - q(x) - q(y)}{2} = \frac{q(x+y) - q(x-y)}{4}.$$

En particulier, on voit que l'ensemble des formes quadratiques q sur V est un K-espace vectoriel isomorphe au K-espace vectoriel des formes bilinéaires symétriques de V. Il est de dimension $\frac{n(n+1)}{2}$.

On a de plus les définitions équivalentes suivantes :

Proposition 5.1. *Soit V un espace vectoriel de dimension finie sur K. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base fixée de V et $q : V \to K$ une application. Les assertions suivantes sont équivalentes :*

(1) L'application q est un polynôme homogène de degré 2, i.e. il existe des formes linéaires $(\ell_1, \dots, \ell_p)$ et $(\ell'_1, \dots, \ell'_p)$ de V telles que $q = \sum_{i=1}^{p} \ell_i \ell'_i$.

(2) Il existe une matrice symétrique A telle que pour tout x de V, on a $q(x) = {}^t xAx$. En écrivant $A = (a_{i,j})_{1 \leq i,j \leq n}$ et $x = \sum_{i=1}^{n} x_i e_i$, l'équation devient $q(x) = \sum_{i,j} a_{i,j} x_i x_j$.

(3) q est une forme quadratique, i.e. il existe une forme bilinéaire symétrique b_q de V telle que $q(x) = b_q(x, x)$ pour tout x de V.

Démonstration. Soit $(e_1^*, \dots, e_n^*)$ la base duale de $\mathcal{B}$. On voit que (2) implique (1) en prenant $\ell_i = e_i^*$ et $\ell'_i = \sum_{j=1}^{n} a_{i,j} e_j^*$ et (2) implique (3) en posant $b(x, y) = \sum_{i,j} a_{i,j} x_i y_j$.

Montrons que (1) implique (2). En écrivant les formes linéaires dans la base duale $(e_1^*, \dots, e_n^*)$ et en développant les produits $\ell_k \ell'_k$, on voit que $q(x)$ peut s'écrire sous la forme $q(x) = \sum_{1 \leq i \leq j \leq n} b_{i,j} x_i x_j$ acec $b_{i,j}$ dans K ne dépendant que des formes linéaire ℓ_k et ℓ'_k. On définit $a_{i,i} := b_{i,i}$ et $a_{i,j} = \frac{b_{i,j}}{2}$ si $i \neq j$ et on obtient de cette façon la matrice symétrique A voulue.

Montrons que (3) implique (2). Puisqu'on peut écrire $b(x, y) = \sum_{i,j} a_{i,j} x_i x_j$ avec $a_{i,j}$ dans K, on obtient (2) en considérant la matrice associée aux $a_{i,j}$. Puisque b est symétrique, la matrice A est symétrique. □

5.2 Classes de congruence

On note $\mathcal{S}_n(K)$ l'espace des matrices symétriques de taille $n \times n$ sur K.

(•) Action de congruence.

Le groupe $\mathrm{GL}_n(K)$ agit sur $\mathcal{S}_n(K)$ via

$$\forall g \in \mathrm{GL}_n(K),\ \forall A \in \mathcal{S}_n(K), \quad g \cdot A = gA^t g.$$

On appelle classes de congruence les orbites de cette action.

Lemme 5.2. *Deux matrices symétriques A et A' sont congruentes si et seulement si elles représentent la même forme quadratique q.*

Démonstration. Soit q une forme quadratique sur un espace V et $\mathcal{B}$ une base de V telle que $A = \mathrm{Mat}_{\mathcal{B}}(q)$. Supposons qu'il existe P dans $\mathrm{GL}_n(K)$ tel que $A' = {}^t PAP$. Soit $\mathcal{B}'$ la base de V obtenue en multipliant la base $\mathcal{B}$ par P. Si x est un vecteur de V qui a pour coordonnées X dans $\mathcal{B}$ et X' dans $\mathcal{B}'$ alors $X = PX'$ et on obtient

$${}^t X' A' X' = {}^t X'^t PAPX' = {}^t XAX = q(x)$$

et donc A' représente bien la forme q.

Réciproquement, si A et A' représentent toutes les deux la forme q dans deux bases différentes $\mathcal{B}$ et $\mathcal{B}'$, alors pour tout vecteur x, on a

$$^tX'A'X' = q(x) = {}^tXAX = {}^tX'{}^tPAPX'$$

et donc $A' = {}^tPAP$. □

(•) Invariants pour l'action de congruence.

Notons que si A et A' sont dans la même classe de congruence alors elles ont même rang (puisqu'elles sont alors équivalentes). De plus on a :

$$\det(A) = \det(P)^2\det(A')$$

et on voit alors que la classe du déterminant de A modulo les carrés est égale à celle du déterminant de A'. On appelle donc rang d'une forme quadratique le rang d'une matrice qui la représente et discriminant d'une forme quadratique la classe modulo les carrés du déterminant d'une matrice qui la représente. On notera $\mathrm{rg}(q)$ (ou $\mathrm{rg}(A)$) et $\delta(q)$ (ou $\delta(A)$) ces invariants.

Dans le cas où $q : V \to \mathbf{R}$ est une forme quadratique sur $\mathbf{R}$, on peut aussi définir l'invariant suivant :

$$p(q) := \max\{\dim(W) \mid W \subset V \text{ tel que pour } x \in W \setminus \{0\},\ q(x) > 0\}.$$

(•) Existence de bases orthogonales.

Théorème 5.3. *Soit q une forme quadratique sur un K-espace vectoriel de dimension finie V. Alors il existe une base dans laquelle la matrice de q est diagonale.*

Démonstration. On prouve le résultat par récurrence sur la dimension n de l'espace V. Pour $n = 1$, c'est évident. Soit alors $n \geq 2$ tel que le résultat est vrai pour $n-1$ et soit q une forme quadratique sur V de dimension n. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de V et $A = (a_{i,j})$ la matrice de q dans $\mathcal{B}$. Pour $x = (x_i)$, on a donc

$$q(x) = \sum_{i=1}^{n} a_{i,i}x_i^2 + \sum_{i<j} 2a_{i,j}x_ix_j.$$

Si $a_{1,j} = 0$ pour tout j, il suffit d'utiliser l'hypothèse de récurrence pour obtenir une base $(f_2, \ldots, f_n)$ du K-espace vectoriel $V' := \mathrm{Vect}(e_2, \ldots, e_n)$ telle que $q|_{V'}$ est diagonale dans $(f_2, \ldots, f_n)$: la base $(e_1, f_2, \ldots, f_n)$ convient alors.

Supposons maintenant que $a_{1,1} \neq 0$. On écrit

$$q(x) = a_{1,1}(x_1 + \sum_{j=2}^{n} \frac{a_{1,j}}{a_{1,1}}x_j)^2 + \widetilde{q}(x)$$

où $\widetilde{q}$ est une forme quadratique telle que $\widetilde{q}(e_1) = 0$. On applique l'hypothèse de récurrence pour obtenir une base $(f_2, \dots, f_n)$ du K-espace vectoriel $V' := \mathrm{Vect}(e_2, \dots, e_n)$ telle que $\widetilde{q}|_{V'}$ est diagonale dans $(f_2, \dots, f_n)$. On considère la base duale $(e_1^*, f_2^*, \dots, f_n^*)$ de $(e_1, f_2, \dots, f_n)$. On peut alors écrire :

$$q(x) = a_{1,1}(x_1 + \sum_{j=2}^{n} \frac{a_{1,j}}{a_{1,1}} x_j)^2 + \sum_{j=2}^{n} \alpha_j f_j^*(x)^2.$$

En posant $f_1^* := e_1^* + \sum_{j=2}^{n} \frac{a_{1,j}}{a_{1,1}} e_j^*$, on a donc bien que la base $(f_1, f_2, \dots, f_n)$ diagonalise q.

Supposons enfin que $a_{1,1} = 0$ et qu'il existe $j \neq 1$ tel que $a_{1,j}$ est non nul. Quitte à permuter deux vecteurs de la base, on peut supposer que c'est $a_{1,2}$. On écrit q sous la forme :

$$q(x) = 2a_{1,2}x_1x_2 + x_1\ell_1(x) + x_2\ell_2(x) + q_0(x)$$

où ℓ_1 et ℓ_2 sont des formes linéaires sur l'espace $\mathrm{Vect}(e_3, \dots, e_n)$ et q_0 est une forme quadratique sur l'espace $\mathrm{Vect}(e_3, \dots, e_n)$. En posant $b := 2a_{1,2}$ on obtient

$$\begin{aligned} q(x) &= b(x_1 + \frac{1}{b}\ell_2(x))(x_2 + \frac{1}{b}\ell_1(x)) - \frac{1}{b}\ell_1(x)\ell_2(x) + q_0(x) \\ &= \frac{b}{4}\big(x_1 + x_2 + \frac{\ell_1(x)}{b} + \frac{\ell_2(x)}{b}\big)^2 - \frac{b}{4}\big(x_1 - x_2 - \frac{\ell_1(x)}{b} + \frac{\ell_2(x)}{b}\big)^2 + q_1(x), \end{aligned}$$

où $q_1 = -\frac{\ell_1\ell_2}{b} + q_0$ est une forme quadratique sur l'espace $\mathrm{Vect}(e_3, \dots, e_n)$. On pose ensuite

$$f_1^* = e_1^* + e_2^* + \frac{\ell_1}{b} + \frac{\ell_2}{b}, \quad f_2^* = e_1^* - e_2^* - \frac{\ell_1}{b} + \frac{\ell_2}{b} \quad \text{et} \quad f_j^* = e_j^* \text{ pour } j \geq 3.$$

Puis, par récurrence, on peut diagonaliser q_1 dans une base dont les vecteurs sont obtenus comme des combinaisons linéaires des $f_j^*, j \geq 3$. Ceci termine la preuve du théorème.

□

Remarque 5.4. La matrice diagonale obtenue via le calcul ci-dessus n'est pas unique. Par exemple, les matrices diagonales $\mathrm{diag}(a, b)$ et $\mathrm{diag}(a + b, (a + b)ab)$ sont congruentes. En effet on a

$$\begin{pmatrix} 1 & 1 \\ b & -a \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & b \\ 1 & -a \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & (a+b)ab \end{pmatrix}$$

5.3 Classification des formes quadratiques

Quand on travaille sur les corps classiques, les invariants de congruence définis ci-dessus sont en fait des invariants totaux. Plus précisément, on a les théorèmes de classification suivants.

(•) Classification des formes quadratiques sur $\mathbf{R}$ et sur $\mathbf{C}$.

Théorème 5.5. *(1) Si $K = \mathbf{C}$, deux matrices A, A' de $\mathcal{S}_n(\mathbf{C})$ sont congruentes si et seulement si elles ont le même rang :* $\mathrm{rg}(A) = \mathrm{rg}(A')$.

(2) Si $K = \mathbf{R}$, deux matrices A, A' de $\mathcal{S}_n(\mathbf{R})$ sont congruentes si et seulement si elles ont le même rang et même invariant p : $\mathrm{rg}(A) = \mathrm{rg}(A')$ *et* $p(A) = p(A')$.

Démonstration. On sait déjà que le rang et p sont des invariants pour les classes de congruence. Il suffit donc de montrer que toutes les matrices A ayant les mêmes invariants sont congruentes à la même matrice qu'on appellera "forme normale" de q. On utilise pour cela l'algorithme d'orthogonalisation proposé dans la preuve du Théorème 5.3.

(1) On suppose que $K = \mathbf{C}$. Soit A dans $\mathcal{S}_n(\mathbf{C})$ de rang $r \neq 0$ qui représente une forme quadratique $q : V \to \mathbf{C}$. Par le Théorème 5.3, on sait qu'il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de V tel que $\mathrm{Mat}_{\mathcal{B}}(q)$ est diagonale. Si $q(e_i) = 0$, on pose $f_i := e_i$ et sinon, on pose $f_i := \frac{1}{\lambda_i} e_i$ où $\lambda_i^2 = q(e_i)$ (rappelons qu'on travaille sur $\mathbf{C}$). On obtient donc bien une base $(f_1, \ldots, f_n)$ telle que $q(f_i) = 1$ ou 0. Quitte à permuter les vecteurs de la base, on obtient que A est congruente à une matrice de la forme :

$$\begin{pmatrix} \mathbf{1}_k & 0 \\ 0 & 0 \end{pmatrix}.$$

De plus, puisque A est de rang r, on a nécessairement $k = r$.

(2) On suppose que $K = \mathbf{R}$. Soit A dans $\mathcal{S}_n(\mathbf{R})$ de rang r et de p-invariant $p(A) = p$, et qui représente une forme quadratique $q : V \to \mathbf{R}$. On note $q := r - p$. Par le Théorème 5.3, on sait qu'il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de V tel que $\mathrm{Mat}_{\mathcal{B}}(q)$ est diagonale. Si $q(e_i) = 0$, on pose $f_i := e_i$. Si $q(e_i) > 0$, on pose $f_i := \frac{1}{\lambda_i} e_i$ où $\lambda_i^2 = q(e_i)$ de sorte à avoir $q(f_i) = 1$. Si $q(e_i) < 0$, on pose $f_i := \frac{1}{\lambda_i} e_i$ où $\lambda_i^2 = -q(e_i)$de sorte à avoir $q(f_i) = -1$. Quitte à permuter les vecteurs de la base, on obtient que A est congruente à une matrice de la forme :

$$A' := \begin{pmatrix} \mathbf{1}_{k_1} & 0 & 0 \\ 0 & -\mathbf{1}_{k_2} & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Montrons qu'on a $p(A') = k_1$. Soit W est un sous-espace de V de dimension d avec $d > k_1$, on veut montrer qu'il existe $x \neq 0$ dans W tel que $q(x) \leq 0$. On considère $W_1 := \mathrm{Vect}(f_{k_1+1}, \cdots, f_n)$ (où $(f_1, \cdots, f_n)$ est la base qui permet d'écrire q sous la forme de A'). On a donc $q(y) \leq 0$ pour tout y de W_1. On est ramené à montrer que $W \cap W_1 \neq \{0\}$. Mais par la formule de Grassmann on a :

$$\dim(W \cap W_1) = \dim(W) + \dim(W_1) - \dim(W + W_1) \geq k_1 + 1 + n - k_1 - n = 1,$$

ce qui montre que $W \cap W_1 \neq \{0\}$ et donc il existe $x \neq 0$ dans W tel que $q(x) \leq 0$. On a donc bien $p(A') \leq k_1$. Puis $p(A') = k_1$ car il suffit de considérer l'espace engendré par $(f_1, \ldots, f_{k_1})$ pour obtenir un espace sur lequel $q > 0$.

Puisque l'invariant p ne dépend que de q et pas de sa matrice représentative, on en déduit que $p = k_1$. De même, puisque le rang est invariant sur les classes de congruence on a $k_1 + k_2 = r = p + q$ et donc $k_2 = q$.

□

On peut reformuler de la manière suivante :

Théorème 5.6. *Soit q une forme quadratique.*

(1) Si $K = \mathbf{C}$, il existe une base orthogonale $\mathcal{B}$ telle que $\mathrm{Mat}_{\mathcal{B}}(q) = \mathrm{diag}(1, \dots, 1, 0, \dots, 0)$ où le nombre de 1 est donné par le rang de q.

(2) Si $K = \mathbf{R}$, il existe une base orthogonale $\mathcal{B}$ telle que $\mathrm{Mat}_{\mathcal{B}}(q) = \mathrm{diag}(1, \dots, 1, -1, \dots, -1, 0, \dots, 0)$ où le nombre p de 1 et le nombre q de -1 vérifient $p + q = \mathrm{rg}(q)$.

Dans le cas réel, la paire (p, q) est appelée la signature de q.

Exemple 5.7. Considérons la forme quadratique sur K^2 représentée dans la base canonique par la matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. On a $\det(A) = -1$ donc la matrice est de rang 2. Si $K = \mathbf{C}$, on a donc $A \simeq \mathbf{1}_2$. En effet on peut vérifier que le procédé décrit ci-dessus donne :

$$2xy = \Big(\frac{x+y}{\sqrt{2}}\Big)^2 + \Big(\frac{i(x-y)}{\sqrt{2}}\Big)^2.$$

Si $K = \mathbf{R}$, la matrice A est congruente à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ (c'est la seule possibilité puisqu'on veut une matrice de discriminant -1). La forme quadratique associée est de signature $(1, 1)$. On vérifie qu'on a bien :

$$2xy = \Big(\frac{x+y}{\sqrt{2}}\Big)^2 - \Big(\frac{(x-y)}{\sqrt{2}}\Big)^2.$$

(•) Classification des formes quadratiques sur $\mathbf{F}_q$.

Théorème 5.8. *Soit V un espace vectoriel de dimension finie sur un corps fini $\mathbf{F}_q$ de caractéristique différente de 2. Soit q une forme quadratique sur V. Pour a dans $\mathbf{F}_q$ qui n'est pas un carré, il existe une base dans laquelle la matrice de q est de la forme $\mathrm{diag}(0, \dots, 0, 1, \dots, 1)$ ou $\mathrm{diag}(0, \dots, 0, 1, \dots, 1, a)$.*

Avant de prouver le théorème, commençons par montrer les résultats suivants :

Lemme 5.9. *L'ensemble $H := \{x^2 \mid x \in \mathbf{F}_q^\times\}$ est un sous-groupe d'indice 2 de $\mathbf{F}_q^\times$, i.e. on a la décomposition $\mathbf{F}_q^\times = H \cup aH$ pour tout non carré $a \in \mathbf{F}_q^\times$. En particulier, il y a exactement $\frac{q+1}{2}$ carrés dans $\mathbf{F}_q$.*

Démonstration. On considère le morphisme de groupe $\varphi : x \mapsto x^2$ de $\mathbf{F}_q^\times$ dans lui-même. Son noyau est égal à $\{\pm 1\}$ qui est d'ordre 2 puisque la caractéristique de $\mathbf{F}_q$ est différente de 2. Ainsi $H = \mathrm{Im}(\varphi)$ est d'indice 2. Il contient donc $\frac{q-1}{2}$ éléments et en ajoutant 0, on voit qu'il y a bien $\frac{q+1}{2}$ carrés dans $\mathbf{F}_q$. □

Corollaire 5.10. *Pour $a, b \neq 0$ dans $\mathbf{F}_q$, l'équation $ax^2 + by^2 = 1$ admet toujours des solutions $(x, y) \neq (0, 0)$.*

Démonstration. On considère les parties $\{\frac{1-by^2}{a}, y \in \mathbf{F}_q\}$ et $\{x^2, x \in \mathbf{F}_q\}$. On a vu dans le lemme précédent qu'elles sont de cardinal $\frac{q+1}{2}$. Leur intersection est donc nécessairement non trivial et on vérifie facilement que 0 n'est pas dans l'intersection. Donc il existe x et y non nuls tels que $ax^2 + by^2 = 1$. □

Preuve du Théorème 5.8. Soit A une matrice symétrique de $\mathcal{S}_n(\mathbf{F}_q)$, de rang r. Notons $q : \mathbf{F}_q^n \to \mathbf{F}_q$ la forme quadratique associée. Soit a dans $\mathbf{F}_q$ qui n'est pas un carré. On écrit $\mathbf{F}_q^\times = H \cup aH$ où H est l'ensemble des carrés de $\mathbf{F}_q^\times$.

Par le Théorème 5.3, on sait qu'il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de V tel que $\mathrm{Mat}_{\mathcal{B}}(q)$ est diagonale. Si $q(e_i) = 0$, on pose $f_i := e_i$. Si $q(e_i)$ est dans H, on pose $f_i := \frac{1}{\lambda_i} e_i$ où $\lambda_i^2 = q(e_i)$ de sorte que $q(f_i) = 1$. Si $q(e_i)$ est dans aH, on pose $f_i := \frac{1}{\lambda_i} e_i$ où $a\lambda_i^2 = q(e_i)$ de sorte que $q(f_i) = a$. On obtient que A est congruente à $\mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_r, 0 \ldots, 0)$ où $\varepsilon_i \in \{1, a\}$.

On peut raffiner encore la matrice diagonale. Par le corollaire 5.10, on sait que pour tout $1 \leq i \leq r-1$, il existe une paire $(x_{i,i}, x_{i,i+1}) \neq (0, 0)$ telle que

$$\varepsilon_i x_{i,i}^2 + \varepsilon_{i+1} x_{i,i+1}^2 = 1.$$

En posant $\widetilde{f_i} := x_{i,i} f_i + x_{i,i+1} f_{i+1}$ pour $1 \leq i \leq r-1$ et $\widetilde{f_i} = f_i$ pour $i \geq r$, on obtient que A est congruente à la matrice $\mathrm{diag}(1, \ldots, 1, \varepsilon_r, 0 \ldots, 0)$ avec $\varepsilon_i \in \{1, a\}$. Quitte à permuter la base, on voit que A est soit congruente à la matrice $\mathrm{diag}(0, \ldots, 0, 1, \ldots, 1)$, soit à $\mathrm{diag}(0, \ldots, 0, 1, \ldots, 1, a)$. □

Si on note b_q la forme bilinéaire symétrique associée à q et qu'on définit

$$\mathrm{Ker}(b_q) := \{x \in V \mid b_q(x, y) = 0 \text{ pour tout } y \in V\}$$

alors, on peut définir une forme bilinéaire symétrique $\overline{b}_q$ sur l'espace $V/\mathrm{Ker}(b_q)$ (on note $\overline{q}$ la forme quadratique associée). Alors $\overline{b}_q$ est non-dégénérée. On définit le discriminant réduit $\overline{\delta}(q)$ d'une forme quadratique q comme le discriminant de la forme $\overline{q}$. On a donc montré :

Théorème 5.11. *Si $K = \mathbf{F}_q$, deux matrices A, A' de $\mathcal{S}_n(\mathbf{F}_q)$ sont congruentes si et seulement si elles ont même rang et même discriminant réduit.*

Exemple 5.12. Soit K un corps fini de caractéristique différente de 2. On reprend notre exemple précédent : on considère la forme quadratique sur K^2 représentée dans la base canonique par la matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. On a $\det(A) = -1$ donc A est congruente soit à $\mathbf{1}_2$ soit à $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ selon que -1 est un carré ou non (i.e. selon que $q = 1 \bmod 4$ ou $q = 3 \bmod 4$).