ÉNS de Lyon
M2 FEADéP

Cours d'algèbre
2019–2020

Anneaux, idéaux et polynômes

Leçons directement concernées (2020)

(102)* Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

(120) Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

(122*) Anneaux principaux. Applications.

(141) Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

(142*) PGCD et PPCM, algorithmes de calcul. Applications.

(144)* Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

Leçons liées, dans lesquelles on peut parler d'anneaux, idéaux et anneaux de polynômes(2020)

(105) Groupe des permutations d'un ensemble fini. Applications.

(110)* Structure et dualité des groupes abéliens finis. Applications.

(121) Nombres premiers. Applications.

(123) Corps finis. Applications.

(125)* Extensions de corps. Exemples et applications.

(126*) Exemples d'équations en arithmétique.

(153) Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

(190) Méthodes combinatoires, problèmes de dénombrement.

Leçons où des techniques d'anneaux de polynômes (en plusieurs variables) peuvent apparaître (2020)

(152) Déterminant. Exemples et applications.

(156) Exponentielle de matrices. Applications.

(170) Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

(171)* Formes quadratiques réelles. Coniques. Exemples et applications.

Ce qui est dans le programme

(a) Anneaux (unitaires), morphisme d'anneaux, sous-anneaux. L'anneau $\mathbb{Z}$ des entiers relatifs. Produit d'anneaux. Idéaux d'un anneau commutatif, anneaux quotients, idéaux premiers, idéaux maximaux. Théorème chinois. Notion d'algèbre (associative ou non) sur un anneau commutatif.

(b) Algèbre des polynômes à une ou plusieurs indéterminées sur un anneau commutatif. Racine d'un polynôme, multiplicité. Relations entre les coefficients et les racines d'un polynôme scindé. Sommes de Newton. Polynôme dérivé. Décomposition en somme de polynômes homogènes. Polynômes symétriques.

(d) Divisibilité dans les anneaux commutatifs intègres. Éléments irréductibles, éléments inversibles, éléments premiers entre eux. Anneaux factoriels. Plus grand diviseur commun, plus petit multiple commun. Factorialité de $A[X]$ quand A est un anneau factoriel. Anneaux principaux. Théorème de Bézout. Anneaux euclidiens. Algorithme d'Euclide. Cas de l'anneau $\mathbb{Z}$ et de l'algèbre $K[X]$ des polynômes sur le corps K. Polynômes irréductibles. Exemples : polynômes cyclotomiques dans $\mathbb{Q}[X]$, critère d'Eisenstein.

(e) Congruences dans $\mathbb{Z}$. Nombres premiers. Étude de l'anneau $\mathbb{Z}/n\mathbb{Z}$ et de ses éléments inversibles, fonction indicatrice d'Euler.

(f) Corps des fractions rationnelles à une indéterminée sur un corps. Décomposition en éléments simples. Cas réel et complexe.

Table des matières

Bibliographie

- À suivre...

1 Anneaux commutatifs

1.1 Notions de base

Définition 1.1. Un *anneau unitaire* (ou plus simplement un anneau) $(A, +, \cdot)$ est un ensemble A muni de deux lois de composition internes $+$ et $\cdot$ telles que :

— $(A, +)$ est un groupe abélien (dont on note 0 l'élément neutre) ;

— la loi $\cdot$ est associative et possède un élément neutre, noté 1 ;

— la loi de multiplication $\cdot$ est distributive par rapport à l'addition $+$.

Un *sous-anneau* de A est un sous-groupe B de $(A, +)$ qui contient 1 et qui est stable par multiplication.
Un anneau est dit *commutatif* si $a \cdot b = b \cdot a$ pour tous $a, b \in A$.
Un anneau est dit *intègre* s'il est non nul et si le produit de deux éléments non nuls est non nul.

Remarque 1.2. On évitera de dire que A est un anneau lorsqu'il est non-unitaire, on parlera alors plutôt de pseudo-anneau dans ce cas.

Exemple 1.3.

1. Si $0 = 1$, alors l'anneau est nul et ne contient qu'un élément. En effet, pour tout $a \in A$, on a $a = a \cdot 1 = a \cdot 0 = a \cdot (a + (-a)) = a \cdot a + (-a) \cdot a = a \cdot a - a \cdot a = 0$.
2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs intègres.
3. $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif non intègre.
4. $\mathbb{N}$ n'est pas un anneau.
5. Si A est un anneau commutatif, alors $A[X]$ est un anneau commutatif et $\mathcal{M}_n(A)$ est un anneau non commutatif pour $n \geq 2$.

Définition 1.4. Un *morphisme d'anneaux* est une application $f : A \to B$ telle que :

— $f(a + b) = f(a) + f(b)$;

— $f(ab) = f(a)f(b)$;

— $f(1) = 1$.

Exemple 1.5.

1. Si B est un sous-anneau de A, alors l'inclusion $B \to A$ est un morphisme d'anneaux ; typiquement $\mathbb{Z} \to \mathbb{Q}$.
2. Si A anneau commutatif et $a \in A$, on a des morphismes d'évaluation en a donnés par : $\mathrm{ev}_a : P \in A[X] \mapsto P(a)$

Définition 1.6. Soient $a, b \in A$ deux éléments.
On dit que b *divise* a et on note $b|a$ s'il existe $c \in A$ tel que $a = bc$.
Un élément a d'un anneau A est dit :

— *inversible* s'il existe $b \in A$ tel que $ab = 1$, on note $A^\times$ l'ensemble des éléments inversibles de $A^\times$;

— *irréductible* si $a \notin A^\times$ et si $a = bc$ implique que $b \in A^\times$ ou $c \in A^\times$;

— *premier* si $a \notin A^\times$ et si $a|bc$ implique que $a|b$ ou $a|c$ – lorsque A est commutatif ;

— *diviseur de* 0 si $a \neq 0$ et s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$;

— *nilpotent* si $a^n = 0$ pour un certain $n \in \mathbb{N}^*$;

— *idempotent* si $a^2 = a$.

Un *corps* est un anneau commutatif dans lequel tout élément est inversible.

Fait 1.7. *L'ensemble $A^\times$ est un groupe pour $\cdot$.*
Si A est intègre, alors :

— *0 est le seul élément nilpotent,*

— *1 est le seul élément idempotent,*

— *A n'admet pas de diviseurs de 0,*

— *tout élément premier est irréductible.*

Exemple 1.8. Dans $\mathbb{Z}/6\mathbb{Z}$, l'élément 3 est premier mais il est idempotent donc pas irréductible.
Dans $A = \mathbb{Z}[i\sqrt{5}]$, l'élément 2 est irréductible mais n'est pas premier car $2 \cdot 3 = \left(1 - i\sqrt{5}\right)\left(1 + i\sqrt{5}\right)$.

Fait 1.9. *Pour tout $a \in A$, on a $1 \mid a \mid 0$.*

Le groupe $A^\times$ agit par multiplication à droite sur A. On note $A/A^\times$ l'espace des orbites.

Si A est intègre, alors la relation binaire $\cdot \mid \cdot$ est une relation d'ordre partielle sur $A/A^\times$ pour laquelle 1 est le plus petit élément et 0 est le plus grand élément.

Ces deux faits très élémentaires seront un très bon exercice pour le lecteur qui voudra se familiariser avec les définitions.

Remarque 1.10. Lorsque l'anneau A n'est pas intègre, il se peut qu'il y ait des diviseurs de 0 et que $\cdot \mid \cdot$ ne soit pas une relation d'ordre.

Par exemple, pour $A = \mathbb{Z}/6\mathbb{Z}$, l'élément 2 est un diviseur de 0 mais 2 et 0 n'ont pas la même orbite.

Exercice 1. Soit K un corps. Trouvez les éléments inversibles, irréductibles, premiers, diviseurs de 0, nilpotents, idempotents des anneaux suivants :

$$\mathbb{Z}/n\mathbb{Z}, \qquad K, \qquad K[X], \qquad \mathcal{M}_2(K).$$

1.2 Idéaux

Dans toute la suite A est un anneau commutatif.

Il existe une notion d'idéal à gauche, à droite, bilatère dans un anneau non-commutatif mais nous n'en parlerons pas.

Définition 1.11. Un *idéal* I de A est un sous-A-module de A, autrement dit un sous-groupe de $(A, +)$ tel que pour tout $a \in A$ et tout $i \in I$, on a $a \cdot i \in I$.

Fait 1.12. *Une intersection quelconque et une réunion croissante d'idéaux forment des idéaux de A.*

Définition 1.13. Si X est une partie de A, on appelle *idéal engendré par X* le plus petit idéal de A contenant X, qu'on peut réaliser comme intersection de tous les idéaux de A contenant X.

Si $X = \{a_1, \dots, a_n\}$ on notera souvent $(a_1, \dots, a_n)$ l'idéal engendré par X.

Fait 1.14. *Si I et J sont des idéaux, on note :*

- *$I + J = \{i + j,\ i \in I,\ j \in J\}$ est l'idéal de A engendré par $I \cup J$;*
- *$I \cdot J$ l'idéal engendré par la famille $(i \cdot j)_{i \in I,\ j \in J}$.*

Définition 1.15. On dit que I et J sont *premiers entre eux* si $I + J = A$.

Fait 1.16. *Si I est un idéal de A alors le groupe $B = A/I$ est un anneau et le morphisme de groupes $\pi : A \to B$ est un morphisme d'anneaux.*

Les idéaux de A sont les noyaux $\ker f$ *des morphismes d'anneaux $f : A \to C$.*

Remarque 1.17. On évitera de parler de somme quelconque d'idéaux. Si $(I_x)_{x \in X}$ sont des idéaux de A, on pourra poser $J = \sum_{x \in X} I_x = \left\{ \sum_{y \in Y} i_y,\ i_y \in I_y \text{ et } Y \subset X \text{ partie finie} \right\}$. En général, J est un idéal de A distinct de l'idéal engendré par les I_x.

Définition 1.18. Un idéal I de A est dit :

- *propre* si $I \neq A$;
- *premier* si s'il est propre et si $xy \in I$ entraîne $x \in I$ ou $y \in I$;
- *maximal* s'il est propre et maximal au sens de l'inclusion, autrement dit si I et A sont les seuls idéaux de A contenant I ;
- *principal* s'il est engendré par 1 élément.

Proposition 1.19. *Soit I un idéal de A et $J = (a)$ un idéal principal de A engendré par $a \in A$. Alors :*

1. *I est premier $\iff$ A/I est intègre.*
2. *I est maximal $\iff$ A/I est un corps.*
3. *$J = (a)$ est un idéal premier $\iff$ a est un élément premier.*
4. *$J = (a)$ est un idéal maximal parmi les idéaux propres principaux $\iff$ a est un élément irréductible.*

Démonstration. Ceci est laissé en exercice. On pourra utiliser le morphisme d'anneaux $\pi : A \to A/I$. □

Exemple 1.20. L'élément 2 est irréductible sur $\mathbb{Z}[i\sqrt{5}]$ mais l'idéal (2) n'est pas maximal car l'anneau $\mathbb{Z}[i\sqrt{5}]/(2)$ n'est pas intègre car $\pi\left(1-\sqrt{5}\right)$ et $\pi\left(1+\sqrt{5}\right)$ sont des diviseurs de 0 dans $\mathbb{Z}[i\sqrt{5}]/(2)$. En particulier, la proposition dit que (1) et (2) sont les seuls idéaux principaux de $\mathbb{Z}[i\sqrt{5}]$ contenant (2).

Corollaire 1.21. *Un anneau est intègre (resp. un corps) si, et seulement si,* 0 *est premier (resp. maximal).*

Théorème 1.22 (Théorème de Krull)**.** *(théorème admis) Soit A un anneau commutatif. Alors tout idéal propre est contenu dans un idéal maximal.*

Démonstration. C'est le lemme de Zorn sur l'ensemble des idéaux propres, inductif pour l'inclusion. □

Lemme 1.23. *Soient $I_1, \dots, I_n$ des idéaux de A deux à deux premiers entre eux. Alors pour tout $k \in [\![1, n-1]\!]$, les idéaux $I_1 \cdots I_k$ et I_n sont premiers entre eux.*

Démonstration. On procède par récurrence sur k. On a $I_1 + I_n = A$.
Hérédité : On écrit $A = A \cdot A = (I_1 \cdots I_{k-1} + I_n) \cdot (I_k + I_n)$. Alors $A \subseteq I_1 \cdots I_k + I_n$. □

Théorème 1.24 (Lemme des restes chinois)**.** *Soit A un anneau commutatif, $n \in \mathbb{N}^*$ et $I_1, \dots, I_n$ des idéaux de A deux à deux premiers entre eux. Alors $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$ et on a un isomorphisme canonique $A/I_1 \cap \cdots \cap I_n \simeq A/I_1 \times \cdots \times A/I_n$.*

Démonstration. On procède par récurrence sur n. Si $n = 1$, il n'y a rien à montrer.
Traitons le cas $n = 2$. Alors on peut définit un morphisme d'anneaux $\begin{array}{rccc} \Phi : & A & \to & A/I_1 \times A/I_2 \\ & a & \mapsto & (a \mod I_1, a \mod I_2) \end{array}$. Le noyau de ce morphisme est $I_1 \cap I_2$. Montrons qu'il est surjectif. Soit $1 = i_1 + i_2$ avec $i_k \in I_k$. Alors $\Phi(ai_2 + bi_1) = (a(1-i_1) + bi_1 \mod I_1, ai_2 + b(1-i_2) \mod I_2) = (a \mod I_1, b \mod I_2)$. Par passage au quotient, on en déduit l'isomorphisme. Enfin, notons que $I_1 \cap I_2 = I_1 \cdot I_2$ car si $y \in I_1 \cap I_2$, alors $y = \underbrace{i_1 y}_{\in I_1 I_2} + \underbrace{i_2 y}_{\in I_1 I_2}$ et la réciproque est immédiate.

Hérédité : Supposons $n \geq 3$. Le lemme nous dit que $I_1 \cdots I_{n-1}$ et I_n sont premiers entre eux donc, par hypothèse de récurrence, on a

$$(I_1 \cdots I_{n-1}) \cdot I_n = (I_1 \cap \cdots \cap I_{n-1}) \cap I_n$$

et

$$A/I_1 \cdots I_n \simeq (A/I_1 \cdots I_{n-1}) \times (A/I_n) \simeq A/I_1 \times \cdots \times A/I_{n-1} \times A/I_n.$$

□

Dans le cas $n = 2$, la preuve construit plus précisément un inverse à Φ en utilisant une relation de la forme $1 = i_1 + i_2$. On se demande alors comment construite explicitement, dans un anneau, une telle relation.

On retiendra que :

Corollaire 1.25. *Soit A un anneau et $a, b, u, v \in A$ des éléments tels que $1 = au + bv$. Alors*

$$\begin{array}{rccc} \Phi : & A/(ab) & \to & A/(a) \times A/(b) \\ & x & \mapsto & (x \mod a, x \mod b) \end{array}$$

est un isomorphisme d'anneaux d'inverse

$$\begin{array}{rccc} \Phi : & A/(a) \times A/(b) & \to & A/(ab) \\ & (x \mod a, y \mod b) & \mapsto & (bv)x + (au)y \end{array}$$

1.3 Anneaux euclidiens et principaux

Définition 1.26. Un anneau est *Euclidien* s'il est intègre et s'il admet un *stathme euclidien*, c'est-à-dire une application $\phi : A \setminus \{0\} \to \mathbb{N}$ telle que pour tout $a \in A$, tout $b \in A \setminus \{0\}$ il existe des éléments $(q, r) \in A^2$ tels que $a = bq + r$ et ($r = 0$ ou $\phi(b) > \phi(r)$).

Exemple 1.27. Les anneaux suivants sont Euclidiens pour les stathmes décrits :

1. $\mathbb{Z}$ pour $|\cdot|$;
2. $\mathbb{K}[X]$ si K corps pour deg ;
3. $\mathbb{Z}[i]$ pour $N(a + ib) = a^2 + b^2$;
4. $\mathbb{K}[\![X]\!]$ pour v_X ;
5. $\mathbb{Z}_p$ pour v_p.

Définition 1.28. Un anneau est *principal* s'il est intègre et si tout idéal est principal.

Soit $(a_i)_{i\in I}$ une famille d'éléments de A.

— On appelle *PGCD* un élément $d \in A$ qui engendre l'idéal engendré par les a_i.

— On appelle *PPCM* un élément $m \in A$ qui engendre l'idéal $\bigcap_{i\in I}(a_i)$.

On dit que les $(a_i)_{i\in I}$ sont *premiers entre eux* si $d \in A^\times$.

Exemple 1.29. Les éléments $6, 10, 15 \in \mathbb{Z}$ sont premiers entre eux mais ne sont pas deux à deux premiers entre eux. On a $1 = 6 + 10 - 15$.

Fait 1.30 (Identités de Bézout)**.** *Soit $(a_i)_{i\in[\![1,n]\!]}$ une famille* **finie** *d'éléments de A et $d = \mathrm{pgcd}(a_1, \ldots, a_n)$. Alors il existe des éléments u_i de A tels que $d = u_1a_1 + \ldots u_na_n$.*

Démonstration. $d \in (a_1) + \cdots + (a_n)$. □

Une telle relation s'appelle une relation de Bézout. On verra plus tard que çe type de relation s'avère utile dans la résolution d'équations diophantiennes.

Théorème 1.31. *Un anneau euclidien est principal.*

Démonstration. Soit A un anneau principal et I idéal non nul de A. L'ensemble $N(I \setminus \{0\})$ est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément. Soit $a \in I$ réalisant le minimum. La division euclidienne nous dit alors que pour tout $b \in I$, on a $b \in (a)$. Donc $I = (a)$. □

Définition 1.32 (Caractéristique d'un corps)**.** Soit K un corps. On a un morphisme d'anneaux canonique $\sigma : \mathbb{Z} \to K$. Son image est un sous-anneau de K, donc intègre. Donc son noyau est un idéal premier de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ avec p premier ou $p = 0$. Ce nombre p, noté $\mathrm{car}(K)$ est la caractéristique du corps K.

Théorème 1.33 (Diviseurs élémentaires)**.** *Si A est un anneau principal et si $M \in \mathcal{M}_{r,s}(A)$, alors il existe des entiers $d_1|\ldots|d_n$, uniquement déterminés, et des matrices $P \in \mathrm{SL}_r(A)$ et $Q \in \mathrm{SL}_s(A)$ telles que $PMQ = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ & & d_n \\ 0 & & 0 \end{pmatrix}$.*

Démonstration. Idée pour l'existence : considérer l'ensemble des matrices équivalentes à M et montrer que l'ensemble des premiers coefficient de ces matrices est un élément minimal pour la division. En déduire que c'est en fait le PGCD des coefficients de M, appliquer des opérations élémentaires sur les lignes et colonnes pour se ramener au cas d'une ligne et d'une colonne nulle sauf le premier terme. Conclure par récurrence.

Pour l'unicité, n montre d'abord l'unicité de n, puis on procède par récurrence sur le PPCM de deux diviseurs élémentaires d_n, d'_n en considérant un quotient par l'idéal engendré par p, pour remplacer d_n et d'_n par $\frac{d_n}{p}$ et $\frac{d'_n}{p}$. Le plus simple étant ici d'utiliser la notion de module libre sur un anneau principal, qui n'est plus au programme de l'agrégation depuis quelques années maintenant. □

Remarque 1.34. Dans le cas d'un anneau Euclidien, on a un algorithme explicite de calcul.

Corollaire 1.35 (Structure des groupes abéliens de type fini)**.** *Si G est un groupe abélien de type fini (i.e. engendré par une partie finie), alors il existe des entiers $r, s \in \mathbb{N}$ et $d_1 | \cdots | d_s$, uniquement déterminés, tels que $G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_s\mathbb{Z}$.*

Démonstration. La version « anneaux » de ce résultat consiste surjecter un $\mathbb{Z}$-module libre de type fini sur le groupe G. Plus précisément, si $X = \{x_1, \ldots, x_n\}$ de cardinal n engendre G, alors on pose $M = \mathbb{Z}^n$ et $f(e_i) = x_i$. Comme $\mathbb{Z}^n$ est un module libre, on peut étendre la formule par $\mathbb{Z}$-linéarité pour définir un morphisme surjectif $f : M \to G$ dont on note N le noyau. Le théorème des diviseurs élémentaires nous dit alors qu'on va pouvoir « diagonaliser » N vu comme sous-$\mathbb{Z}$-module de M, c'est-à-dire trouver une base $\mathcal{B} = (b_1, \ldots, b_n)$ de M et des entiers $d_1 | \ldots | d_n$ tels que $(d_i b_i)_{1 \leq i \leq n}$ est une base de N, avec éventuellement $d_i = 0$ à partir d'un certain rang. On a alors $M/N \simeq \mathbb{Z}/d_i\mathbb{Z} \simeq G$. □

1.4 Anneaux factoriels

Relevons tout d'abord deux propriétés remarquables satisfaites, entre autres, par les anneaux principaux.

Définition 1.36. Soit A un anneau. On définit deux propriétés :

(E) $\forall a \in A \setminus \{0\},\ \exists u \in A^\times,\ \exists r \in \mathbb{N},\ \exists p_1, \ldots, p_r \in A$ irréductibles tels que $a = u p_1 \ldots p_r$;

(U) $\forall u, v \in A^\times,\ \forall r, s \in \mathbb{N},\ \forall p_1, \ldots, p_r, q_1, \ldots, q_s \in A$ irréductibles,
on a $u p_1 \ldots p_r = v q_1 \ldots q_s \quad \Rightarrow \quad r = s$ et $\exists \sigma \in \mathfrak{S}_s,\ \forall i \in [\![1, r]\!],\ \exists w_i \in A^\times,\ p_i = w_i q_{\sigma(i)}$.

Un anneau A est dit *factoriel* s'il est **intègre** et s'il vérifie (E) et (U).

Lemme 1.37. *Si A est principal, alors tout irréductible de A est premier.*

Démonstration. Soit $a \in A$ irréductible tel que $a | bc$. Soit $u \in A$ tel que $au = bc$. Soit $d = \mathrm{pgcd}(a, b)$ et $e \in A$ tel que $a = de$. Comme a est irréductible on a $d \in A^\times$ ou $e \in A^\times$. Si $e \in A^\times$, alors $a | d | b$. Si $d \in A^\times$, alors par Bézout, il existe u, v tels que $1 = au + bv$. Alors $a | bcv$ donc $a | acu + bcv = c$. □

Théorème 1.38. *Tout anneau principal est factoriel.*

Démonstration. Pour (E), considérons l'ensemble J des idéaux (a) de A tels que a ne s'écrit pas sous la forme souhaitée. Supposons par l'absurde $J \neq \emptyset$. On observe d'abord que J admet un idéal qui est maximal au sens de l'inclusion dans J. En effet, si ce n'était pas le cas, il existerait une suite strictement croissante $((a_i))$ d'idéaux de J dont la réunion est un idéal de A, disons (b). Mais alors $b \in (a_i)$ pour un certain i, ce qui contredit la stricte croissance de la suite d'idéaux.

Ensuite, soit (a) un élément maximal de J. Comme a ne peut pas être irréductible, il s'écrit $a = bc$ tels qu'on ait des inclusions strictes $(a) \subset (b)$ et $(a) \subset (c)$. Donc $(b), (c) \notin J$ donnent des écritures $b = u p_1 \cdots p_r$ et $c = v q_1 \cdots q_s$, de sorte que $a = uv p_1 \cdots p_r q_1 \cdots q_s$.

Pour (U), on observe que les irréductibles de A sont premiers, ce qui permet d'ôter un facteur et de conclure par récurrence sur le nombre de facteurs. □

Théorème 1.39 (Lemme d'Euclide)**.** *Dans un anneau factoriel, tout élément irréductible est premier.*

Démonstration. Conséquence immédiate de (U). □

Exemple 1.40. L'anneau $\mathbb{Z}[i\sqrt{5}]$ est intègre mais pas factoriel car $2 \cdot 3 = \left(1 - i\sqrt{5}\right)\left(1 + i\sqrt{5}\right)$. L'élément 2 est irréductible mais pas premier.

Proposition-définition 1.41 (Valuation et PGCD,PPCM)**.**

Notons $\mathcal{P}$ l'ensemble des classes d'éléments irréductibles, modulo les inversibles, d'un anneau factoriel A et, par abus, $p \in \mathcal{P}$ le choix d'un représentant pour une classe donnée. Soit $p \in \mathcal{P}$ un élément irréductible (i.e. sa classe).

Alors, pour tout $a \in A \setminus \{0\}$, le nombre de fois où p apparait dans une décomposition de a, ce qui existe par (E), ne dépend pas de cette décomposition, d'après (U). On appelle cette quantité la *valuation p-adique de a* et on la note $v_p(a)$.

L'ensemble des $p \in \mathcal{P}$ tels que $v_p(a) > 0$ est fini et $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ pour un certain $u \in A^\times$.

On définit alors :

$$\mathrm{pgcd}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\min v_p(a_1), \ldots, v_p(a_n)}; \qquad \mathrm{pgcd}(a_1, \ldots, a_n) = \prod_{p \in \mathcal{P}} p^{\max v_p(a_1), \ldots, v_p(a_n)}.$$

Fait 1.42. *Ce sont des opérations associatives (on peut parenthéser comme bon nous semble).*

Notation 1.43. On note parfois $a \wedge b = \text{pgcd}(a,b)$ et $a \vee b = \text{ppcm}(a,b)$. Quand on utilise une notation non standard comme celle-ci, on le dit !

Théorème 1.44 (Lemme de Gauss)**.** *Si A est factoriel, si $a,b,c \in A$ et si* $\text{pgcd}(a,b) = 1$*, alors $a|bc \Rightarrow a|c$.*

Théorème 1.45 (Gauss)**.** *Si A est factoriel, alors $A[X]$ est factoriel.*

Démonstration. On en reparlera plus tard quand on traitera les anneaux de polynômes. □

1.5 Anneaux noethériens (ceci est hors-programme mais parfois utile)

Définition 1.46. Un anneau A est *noethérien* s'il vérifie les conditions équivalentes suivantes :

(i) tout idéal de A est de type fini ;

(ii) toute suite croissante d'idéaux de A est stationnaire ;

(iii) tout ensemble non vide d'idéaux a un élément maximal pour l'inclusion (pas nécessairement un plus grand élément).

Démonstration. C'est un jeu d'écriture laissé en exercice. □

Fait 1.47. *Tout anneau principal est noethérien.*
Un quotient d'un anneau noethérien est noethérien.

Exemple 1.48. L'anneau $K[X_1, \dots, X_n, \dots]$ est intègre mais n'est pas noethérien.

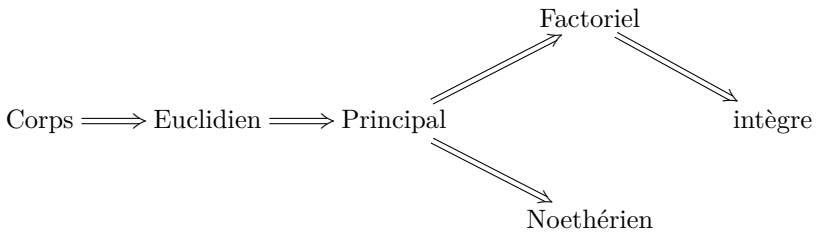
Proposition 1.49. *Si A est un anneau intègre et noethérien, alors il vérifie (E).*

Théorème 1.50 (Hilbert)**.** *Si A est noethérien, alors $A[X]$ est noethérien, donc $A[X_1, \dots, X_n]$ aussi.*

Exemple 1.51. L'anneau $\mathbb{Z}[i\sqrt{5}] \simeq \mathbb{Z}[X]/(X^2+5)$ est noethérien comme quotient d'un anneau noethérien, et intègre en tant que sous-anneau de $\mathbb{C}$. Il vérifie (E), donnez des exemples autres que $6 = 2 \cdot 3$.

Démonstration. Si ça vous intéresse, lisez des livres ! □

Pour résumer les différentes applications et propriétés, traçons le dessin suivant :



Propriétés spécifiques :

— Euclidien : algorithme d'Euclide (calcul explicite de PGCD, PPCM).

— Principal : identités de Bézout.

— Factoriel : (E) et (U) ; irréductible $\Leftrightarrow$ premier ; existence de PGCD, PPCM ; Lemme de Gauss ; Lemme d'Euclide ; existence des valuations p-adiques.

— Noethériens : (E) ; stable par quotient.

— Commutatif : lemme des restes chinois.

Les (contre-)exemples :

— Euclidien : $\mathbb{Z}$, $K[X]$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\frac{1}{10}\right]$, $K[[X]]$, $\mathbb{Z}_p$.

— Principal (non euclidien) : $\mathbb{Z}[(1+i\sqrt{19})/2]$ *(pas facile).*

— Factoriel (et noethérien non principal) : $K[X,Y]$, $\mathbb{Z}[X]$ d'idéaux non principaux (X,Y) et $(2,X)$.

— Noethérien (et intègre non factoriel donc non principal) : $\mathbb{Z}[i\sqrt{5}]$.

— Factoriel (et intègre non noethérien donc non principal) : $K[(X_n), n \in \mathbb{N}]$.

— Intègre (non factoriel, non noethérien) : $\mathcal{H}(\mathbb{C})$ fonctions entières sur $\mathbb{C}$.

2 Polynômes à une indéterminée – compléments

Si A est un anneau, il est en général difficile d'en déterminer les éléments irréductibles (penser par exemple aux irréductibles de $\mathbb{Z}/n\mathbb{Z}$). Lorsque A est un anneau factoriel, les irréductibles jouent alors un rôle important, notamment parce qu'on dispose alors d'une unique écriture en produit d'irréductibles, et donc de valuations associées aux irréductibles de A.

2.1 Permanence de la factorialité

Dans toute la suite, on se restreindra donc au cas d'un anneau factoriel A, donc intègre, dont on notera $K = \mathrm{Frac}(A)$ le corps des fractions.

Définition 2.1. Pour tout polynôme $P = \sum_{i=0}^{d} a_i X^i \in A[X] \setminus \{0\}$, on appelle *contenu* de P, noté $c(P) \in A \setminus \{0\}$, le PGCD dans l'anneau factoriel A des coefficients de P (qui est donc déterminé par le choix d'un système d'irréductibles de A).

On dira que P est *primitif* si $c(P) = 1$.

Lemme 2.2 (Lemme de Gauss sur le contenu)**.** *On suppose A factoriel.*

(1) Pour tout polynôme $P \in A[X] \setminus \{0\}$, il existe un unique $\widetilde{P} \in A[X]$ primitif tel que $P = c(P)\widetilde{P}$.

(2) Si $P, Q \in A[X]$, alors $c(PQ) = c(P)c(Q)$.

(3) Pour tout polynôme $P \in \mathrm{Frac}(A)[X] \setminus \{0\}$, il existe $\alpha \in K^\times$ et $\widetilde{P} \in A[X]$ primitif tel que $P = \alpha\widetilde{P}$. De plus, le couple $\left(\alpha, \widetilde{P}\right)$ est unique à un inversible dans A près, c'est-à-dire que si $P = \alpha Q = \beta R$, alors il existe $\lambda \in A^\times$ tel que $Q = \lambda R$ et $\beta = \lambda\alpha$.

Démonstration. (1) On écrit $P = \sum_{i=0}^{d} a_i X^i$. Pour tout $i \in [\![0, d]\!]$, on peut écrire $a_i = c(P)\widetilde{a_i}$ car $c(P)|a_i$. Le polynôme $\widetilde{P} = \sum_{i=0}^{d} \widetilde{a_i} X^i$ convient. En effet, pour tout $p \in \mathcal{P}$ irréductible de A, on a $v_p(c(P)) = \min\{a_i,\ 0 \leq i \leq d\} = v_p(c(P)) + \min\{\widetilde{a_i},\ 0 \leq i \leq d\} = v_p(c(P)) + v_p(c(\widetilde{P}))$. Donc $v_p(c(\widetilde{P})) = 0$ pour tout irréductible, c'est-à-dire $c(\widetilde{P}) = 1$. L'unicité de $\widetilde{P}$ découle de l'intégrité de l'anneau $A[X]$.

(2) On a $PQ = c(P)c(Q)\widetilde{P}\widetilde{Q}$. Donc $c(PQ) = c(P)c(Q)c(\widetilde{P}\widetilde{Q})$. Il suffit de montrer que $\widetilde{P}\widetilde{Q}$ est primitif.

On écrit $\widetilde{P} = \sum_{i=0}^{d} a_i X^i$ et $\widetilde{Q} = \sum_{j=0}^{e} b_j X^j$ et $\widetilde{P}\widetilde{Q} = \sum_{k=0}^{d+e} c_k X^k$ avec $c_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq d \\ 0 \leq j \leq e}} a_i b_j$.

Soit $p \in A$ un élément irréductible. Il existe un indice minimal i_0 tel que $p \not| a_{i_0}$ et $\forall i < i_0,\ p|a_i$, car sinon, cela signifierait que $p|c(\widetilde{P})$. De même, il existe un indice minimal j_0 tel que $p \not| b_{j_0}$ et $\forall j < j_0,\ p|b_j$. Alors $p|S = \sum_{\substack{i+j=i_0+j_0 \\ i,j \geq 0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j$ et comme $c_{i_0+j_0} = a_{i_0}b_{j_0} + S$, on en déduit que $p \not| c_{i_0+j_0}$.

Par conséquent $p \not| c(\widetilde{P}\widetilde{Q})$. On a donc bien $c(\widetilde{P}\widetilde{Q}) = 1$ et donc $c(PQ) = c(P)c(Q)$.

(3) Existence : Soit $a \in A$ tel que $aP \in A[X]$. Alors par (1), on a $aP = c(aP)\widetilde{aP}$ avec $a \neq 0$ dans K. Ainsi $\alpha = \frac{c(aP)}{a}$ et $\widetilde{P} = \widetilde{aP}$ conviennent.

Unicité : Si $P = \alpha Q = \beta R$ avec $Q, R \in A[X]$ primitifs. Soit $a \in A \setminus \{0\}$ tel que $a\alpha, a\beta \in A$. Alors $c(aP) = c(a\alpha) = c(a\beta)$, donc il existe $\lambda \in A^\times$ tel que $a\beta = \lambda a\alpha$. Par intégrité de A, on a le résultat. □

Insistons sur le fait qu'un choix différent d'un système d'irréductibles définissant un PGCD dans A définit alors un autre contenu avec des égalités à un inversible près dans l'anneau factoriel A.

Proposition 2.3 (Éléments irréductibles de $A[X]$)**.**
Si A est factoriel, alors les polynômes irréductibles de $A[X]$ sont exactement :

- *les polynômes constants, irréductibles dans A ;*
- *les polynômes primitifs non constants irréductibles dans $K[X]$.*

Démonstration. Soit $P \in A[X]$ qu'on écrit $P = QR$ avec $Q, R \in A[X]$.

Si $P = a \in A$ est constant, alors $\deg(Q) + \deg(R) \leq 0$, donc $Q, R \in A$. Comme $A[X]^\times = A^\times$ par additivité des degrés, on en déduit que $a \in A$ est irréductible dans A si, et seulement si, il l'est dans $A[X]$.

Si $\deg(P) \geq 1$, montrons que P est irréductible dans $A[X]$ si, et seulement si, $c(P) = 1$ et P est irréductible dans $K[X]$.

$\Rightarrow$: D'une part, $c(P) = 1$ car sinon, par (1), on aurait que $P = c(P)\widetilde{P}$ est réductible car $c(P), \widetilde{P} \notin A^\times$. D'autre part, si $P = UV$ avec $U, V \in K[X]$, par l'existence de (3), on écrit $U = u\widetilde{U}$ et $V = v\widetilde{V}$ avec $u, v \in K$ et $\widetilde{U}, \widetilde{V} \in A[X]$ primitifs. Alors $P = uv\widetilde{U}\widetilde{V} \in K[X]$ donc, par l'unicité de (3), on a $uv \in A^\times$. Ainsi $\widetilde{U} \in A^\times$ ou $\widetilde{V} \in A^\times$ par irréductibilité de P dans $A[X]$. Mais alors $U \in K^\times$ ou $V \in K^\times$, ce qui nous dit bien que P est irréductible sur $K[X]$.

$\Leftarrow$: Si P est irréductible dans $K[X]$, alors l'écriture $P = QR$ donne en particulier que $Q \in K^\times \cap A = A\backslash\{0\}$ ou $Q \in A\backslash\{0\}$. Comme $c(P) = 1 = c(Q)c(R)$, on a $c(Q) = c(R) = 1$, donc $Q \in A^\times$ ou $R \in A^\times$. □

Théorème 2.4 (Permanence de la factorialité – Gauss)**.** *Si A est factoriel, alors $A[X]$ est factoriel.*

En particulier, tout anneau de polynômes sur un anneau factoriel est factoriel.

Démonstration. Premièrement, $A[X]$ est intègre car A l'est.

Deuxièmement, montrons l'existence (E) d'une décomposition en produit d'irréductibles de tout élément de $A[X]$. Soit $P \in A[X] \setminus \{0\}$ qu'on écrit $P = v\prod_{i\in I} Q_i^{m_i}$ comme produit d'irréductibles Q_i dans $K[X]$ avec $v \in K[X]^\times = K^*$. Pour chaque $i \in I$, on écrit $Q_i = \alpha_i\widetilde{Q_i}$ avec $\alpha_i \in K^*$ et $\widetilde{Q_i} \in A[X]$ primitif, donc irréductible dans $A[X]$ car Q_i l'est dans $K[X]$. Soit $p = v\prod_{i\in I} \alpha_i^{m_i} \in K^*$ et $Q = \prod_{i\in I} \widetilde{Q_i}^{m_i} \in A[X]$ primitif. On a alors $P = c(P)\widetilde{P} = pQ$ et, par unicité de (3), on a $p = \lambda c(P)$ avec $\lambda \in A^\times$. Ainsi $p \in A\backslash\{0\}$ s'écrit $p = u\prod_{j\in J} q_j^{n_j}$ comme produit d'irréductibles dans A, donc dans $A[X]$. Ceci nous donne bien une écriture en produit d'irréductibles de P.

Troisièmement, montrons l'unicité (U) d'une décomposition en produit d'irréductibles de tout élément de $A[X]$. Soit q_j un système d'irréductibles de A qu'on complète en un système d'irréductibles de $A[X]$ par des polynômes de $A[X]$ irréductibles dans $K[X]$ et primitifs P_i. Si P s'écrit de deux manière dans ce système d'irréductibles $P = u\prod_{j\in J} q_j^{n_j}\prod_{i\in I} P_i^{m_i} = v\prod_{j\in J} q_j^{n'_j}\prod_{i\in I} P_i^{m'_i}$ alors, comme les P_i forment encore un système d'irréductibles de $K[X]$, on a, par unicité dans l'anneau Euclidien $K[X]$, que $m_i = m'_i$. Par intégrité de $A[X]$, on a donc $u\prod_{j\in J} q_j^{n_j} = v\prod_{j\in J} q_j^{n'_j}$ dans A, mais alors, par unicité dans l'anneau factoriel A, on a $n_j = n'_j$. □

2.2 Quelques critères d'irréductibilité

On a vu comment ramener l'étude des irréductibles de $A[X]$ à celle des irréductibles de $K[X]$ et de A lorsque A est factoriel. Donnons maintenant des critères d'irréductibilités dans $K[X]$ pour K corps quelconque.

Proposition 2.5 (Sur un corps)**.** *Soit K un corps et $P \in K[X] \setminus \{0\}$. S'équivalent*

(i) P est irréductible ;

(ii) (P) est un idéal premier de $K[X]$;

(iii) (P) est un idéal maximal de $K[X]$;

(iv) $K[X]/(P)$ est un corps.

De plus, si $\deg(P) \leq 3$, ces conditions équivalent à

(v) P est sans racines dans K.

Démonstration. L'anneau $K[X]$ est principal. □

Corollaire 2.6. *Si K est algébriquement clos, les irréductibles de $K[X]$ sont les polynômes de degré 1.*

Voici une généralisation possible de ce corollaire *, qui pourra s'avérer utile dans l'étude des polynômes sur les corps finis :

Proposition 2.7 (Critère par extension)**.** *Soit $P \in K[X]$ tel que $\deg(P) = d \geq 2$. Alors P est irréductible si, et seulement si, dans toute extension de corps L/K de degré $[L : K] \leq \frac{d}{2}$, le polynôme P est sans racines.*

Sur un anneau factoriel, on a déjà vu que :

Proposition 2.8. *$P \in A[X]$ est irréductible si, et seulement si, P est irréductible dans $K[X]$ et $c(P) = 1$.*

∗. On rappelle que toute extension finie d'un corps algébriquement clos est triviale.

Exercice 2.

1. Montrer que $P = X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$ mais qu'il admet une racine sur $\mathbb{F}_{16}$.
2. En déduire une construction de $\mathbb{F}_{16}$ comme corps de rupture sur $\mathbb{F}_2$.

Le plus important des critères d'irréductibilités est le suivant :

Proposition 2.9 (Critère d'Eisenstein)**.** *Soit A un anneau* **factoriel** *et $P = \sum_{i=0}^{d} a_i X^i \in A[X] \setminus \{0\}$. Soit $p \in A$ irréductible. On suppose que :*

— $p \not| a_d$;

— $p | a_i$ *pour tout* $i \in [\![1, d-1]\!]$;

— $p^2 \not| a_0$.

Alors P est irréductible dans $K[X]$.

En particulier, si $c(P) = 1$, alors P est irréductible dans $A[X]$.

Exercice 3. Soit $p \in \mathbb{N}^*$ un nombre premier. Montrer que $\Phi_p = \frac{X^p - 1}{X - 1}$ est irréductible sur $\mathbb{Z}$.

Voici un autre critère d'irréductibilité par réduction :

Proposition 2.10 (Critère par réduction)**.** *Soit A un anneau* **factoriel** *et $K = \mathrm{Frac}(A)$. Soit $P \in A[X]$ de coefficient dominant a_d. Soit I un idéal premier de A et $L = \mathrm{Frac}(A/I)$. On suppose que :*

— $a_d \notin I$;

— *l'image $\overline{P}$ de P dans $L[X]$ est un polynôme irréductible.*

Alors P est irréductible dans $K[X]$.

En particulier, si $c(P) = 1$, alors P est irréductible dans $A[X]$.

Exercice 4. Montrer que le polynôme $X^8Y + XY^2 + Y^2 + Y - 1$ est irréductible dans $\mathbb{Z}[X, Y]$.

Proposition 2.11 (Critère par recherche de racines dans le corps des fractions)**.** *Soit A un anneau factoriel et $K = \mathrm{Frac}(A)$. Soit $P = \sum_{i=0}^{d} a_i X^i \in A[X]$. Si $r = \frac{\alpha}{\beta}$ avec $\alpha, \beta \in A$ tels que $\alpha \wedge \beta = 1$ est une racine de P dans K, alors $\alpha | a_0$ et $\beta | a_d$.*

En particulier, un polynôme P primitif de degré inférieur à 3 est irréductible dans $A[X]$, si et seulement si, il n'admet pas de racines dans $\left\{ \frac{\alpha}{\beta},\ \alpha | a_0 \text{ et } \beta | a_d \right\}$.

Cette dernière condition peut offrir très peu de choses à tester pour vérifier l'irréductibilité d'un polynôme là où le critère d'Eisenstein ne s'applique pas.

Exercice 5. Le polynôme $Q = X^3 - 4X^2 - \frac{9}{2}X - \frac{5}{2}$ est-il irréductible sur $\mathbb{Q}$?

3 Anneaux $\mathbb{Z}/n\mathbb{Z}$ et polynômes cyclotomiques

Pour conclure ce cours de révisions sur les anneaux, étudions l'anneau $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$ est fixé, et ses applications aux polynômes cyclotomiques. Notons $\mathcal{P} \subset \mathbb{N}$ l'ensemble des nombres premiers de $\mathbb{Z}$.

3.1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Cas particulier : Comme $\mathbb{Z}$ est euclidien donc factoriel, les nombres premiers sont également les irréductibles de $\mathbb{Z}$, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, il est intègre et si, et seulement si, n est un nombre premier.

Propriétés d'anneau : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un quotient d'un anneau principal donc tous ses idéaux sont principaux, donc de la forme $(d) = d\mathbb{Z}/n\mathbb{Z}$ avec $d|n$ dans $\mathbb{Z}$. En particulier, tout quotient de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à un $\mathbb{Z}/d\mathbb{Z}$ pour $d|n$.

En revanche, ce n'est ni un anneau principal, ni un anneau factoriel car il n'est pas intègre. On ne dispose donc, entre autres, pas d'un PGCD, PPCM dans $\mathbb{Z}/n\mathbb{Z}$. C'est un anneau fini donc, en particulier noethérien (c'est aussi un quotient d'un anneau noethérien).

Soit $a_1, \dots, a_n$ des éléments de $\mathbb{Z}$, deux à deux premiers entre eux. Le lemme des restes chinois nous donne $\mathbb{Z}/a_1 \dots a_n\mathbb{Z} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$. En particulier, on a :

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{p\in\mathcal{P}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z} \qquad \text{et} \qquad (\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{p\in\mathcal{P}} \left(\mathbb{Z}/p^{v_p(n)}\mathbb{Z}\right)^\times.$$

Il suffit donc de déterminer pour $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$ le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ afin de comprendre le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Indicatrice d'Euler : On observe que pour $a \in [\![1, n-1]\!]$, on a la disjonction :

— soit $a \wedge n \neq 1$ donc a est un diviseur de 0 : en effet $\overline{a} \neq \overline{0}$ et la décomposition en facteurs premiers donne le résultat ;

— soit $a \wedge n = 1$ donc l'identité de Bézout dans $\mathbb{Z}$ donne un inverse à $\overline{a}$ dans $\mathbb{Z}/n\mathbb{Z}$.

On définit *l'indicatrice d'Euler* $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{a \in [\![1, n-1]\!],\ a \wedge n = 1\}$. On pourra remarquer que les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont exactement les éléments qui engendrent chacun le groupe cyclique $(\mathbb{Z}/n\mathbb{Z})$.

Fait 3.1 (Propriétés de l'indicatrice d'Euler)**.**

1. *Si $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$, alors $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*
2. *Si $a \wedge b = 1$, alors $\varphi(ab) = \varphi(a)\varphi(b)$.*
3. *On a $\varphi(n) = n \prod_{\substack{p\in\mathcal{P}\\ p|n}} \left(1 - \frac{1}{p}\right)$.*
4. *On a $n = \sum_{d|n} \varphi(d)$.*

Proposition 3.2 (Quelques applications)**.**

1. *(Théorème d'Euler) Pour tout $a \wedge n = 1$, on a $a^{\varphi(n)} \equiv 1 \mod n$.*
2. *(Théorème de Fermat) Pour tout $p \in \mathcal{P}$ et tout $a \wedge p = 1$, on a $a^{p-1} \equiv 1 \mod p$.*
3. *(Théorème de Wilson) Pour $a \in \mathbb{N}^*$, on a $(a-1)! \equiv -1 \mod a \iff a$ est premier.*
4. *(Théorème RSA) Soient $p, q \in \mathcal{P}$ tels que $p \neq q$ et $n = pq$. Alors pour tous $d, e \in \mathbb{Z}$, on a $de \equiv 1 \mod \varphi(n) \implies \forall m \in \mathbb{Z},\ m^{de} = m \mod n$.*

Structure des $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$:

Théorème 3.3. *Soit $p \in \mathcal{P}$ et $\alpha \in \mathbb{N}^*$.*

1. *On suppose $p \neq 2$. Alors le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique d'ordre $p^{\alpha-1}(p-1)$.*
2. *On suppose $p = 2$.*
   (a) *Si $\alpha \in \{1, 2\}$ alors le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique d'ordre α.*
   (b) *Si $\alpha \geq 3$, alors le groupe $U(\alpha) = \left\{\overline{a} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times,\ a \equiv 1 \mod 4\right\}$ est cyclique, d'ordre $2^{\alpha-2}$ et engendré par $\overline{5}$. De plus, on a un isomorphisme de groues : $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \left\{\overline{\pm 1}\right\} \times U(\alpha)$.*

3.2 Racines de l'unité

Les racines de l'unité ont un intérêt particulier : par exemple, les valeurs propres qui apparaissent dans une représentation linéaire complexe d'un groupe fini, les éléments non nuls d'un corps finis sont des exemples de racines de l'unité.

On va introduire une famille de polynôme qui permet de mieux les appréhender.

Tout d'abord, remarquons que l'ensemble des nombres complexes de modules 1 forme un groupe, souvent noté $\mathbb{U}$ ou $U_1(\mathbb{C})$, naturellement isomorphe à $\mathrm{SO}_2(\mathbb{R})$, commutatif. L'ensemble des éléments d'ordre fini forme un sous-groupe appelé groupe des racines de l'unité dans $\mathbb{C}$.

Définition 3.4. Plus généralement, si K est un corps, on note $\mu(K)$ l'ensemble des racines de l'unité de $K^\times$, autrement dit, l'ensemble des éléments d'ordre fini de $\mathbb{K}^\times$. C'est un sous-groupe, donc commutatif, de $K^\times$.

On note $\mu_n(K) = \{\zeta \in K,\ \zeta^n = 1\}$ le *groupe des racines n-èmes de l'unité* dans K. C'est aussi l'ensemble des éléments de $\mu(K)$ dont l'ordre **divise** n.

On appelle *racine primitive n-ème de l'unité* un élément d'ordre n de $\mu_n(K)$, ce qui n'existe pas toujours. On note $\mu_n^*(K)$ l'ensemble formé par ces racines : celui-ci n'est pas un groupe !

Fait 3.5. *Par définition, on a* $\mu_n(K^\times) = \bigsqcup_{d|n} \mu_d^*(K^\times)$.

Théorème 3.6. *Soit K un corps. Tout sous-groupe fini de $K^\times$ est cyclique.*

Démonstration. Soit $G \subset K^\times$ un groupe fini d'ordre n. Soit $h \in K^\times$ un élément d'ordre $d \in \mathbb{N}^*$. Alors le polynôme $P = X^d - 1$ admet d racines distinctes, donc il est scindé à racines simples et ses racines sont exactement les éléments du sous-groupe H de $K^\times$ engendré par h. Donc le nombre $N(d)$ d'éléments d'ordre d de $K^\times$ est inférieur ou égal au nombre d'éléments d'ordre d de $H \simeq \mathbb{Z}/d\mathbb{Z}$, donc $N(d) \leq \varphi(d)$. On a donc $n = |G| \leq \sum_{d|n} N(d) \leq \sum_{d|n} \varphi(d) = n$. L'égalité est réalisée et, en particulier $N(n) = \varphi(n) \geq 1$. Donc le groupe G d'ordre n admet au moins un élément d'ordre n, ce qui conclut. □

Corollaire 3.7. *Le groupe $\mu_n(K)$ des racines n-èmes de l'unité est cyclique.*

Exemple 3.8.

Cas complexe :

— $\mu_n(\mathbb{C}) = \left\{\zeta_k = e^{\frac{i2\pi k}{n}},\ k \in [\![0, n-1]\!]\right\} \simeq \mathbb{Z}/n\mathbb{Z}$,

— $\mu_n^*(\mathbb{C}) = \left\{\zeta_k = e^{\frac{i2\pi k}{n}},\ k \in [\![0, n-1]\!],\ k \wedge n = 1\right\}$ s'identifie à $(\mathbb{Z}/n\mathbb{Z})^\times$. En particulier, il y a $\varphi(n)$ racines primitives n-èmes de l'unité dans $\mathbb{C}$.

Cas réel ou rationnel :

— $\mu_n(\mathbb{Q}) = \mu_n(\mathbb{R}) = \begin{cases} \{\pm 1\} & \text{si } n \text{ est pair} \\ \{1\} & \text{sinon.} \end{cases}$,

— $\mu_n^*(\mathbb{Q}) = \mu_n^*(\mathbb{R}) = \begin{cases} 1 & \text{si } n = 1 \\ -1 & \text{si } n = 2 \\ \emptyset & \text{si } n \geqslant 3 \end{cases}$.

Cas d'un corps fini $K = \mathbb{F}_q$: Tous les éléments de $\mathbb{F}_q^\times$ sont des racines de l'unité. On a alors $\mu(K) = \mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. On remarque alors que pour d divisant $q-1$, le nombre $\varphi(d)$ est alors le nombre de racines primitives d-èmes de l'unité dans $\mathbb{F}_q^\times$. Ainsi

$$\operatorname{Card} \mu_n^*(\mathbb{F}_q^\times) = \begin{cases} 0 & \text{si } d \not| q-1 \\ \varphi(d) & \text{si } d | q-1 \end{cases}$$

À ce stade, on ne sait pas encore vraiment décrire $\mathbb{F}_q$. On sait dire, néanmoins que

$$\mu_n(\mathbb{F}_q^\times) = \bigsqcup_{d|n} \mu_d^*(\mathbb{F}_q^\times) = \bigsqcup_{\substack{d|n \\ d|q-1}} \mu_d^*(\mathbb{F}_q^\times) = \mu_{\operatorname{pgcd}(n,q-1)}(\mathbb{F}_q^\times)$$

est un groupe cyclique d'ordre $\sum_{d|\operatorname{pgcd}(n,q-1)} \varphi(d) = \operatorname{pgcd}(n, q-1)$.

Remarque 3.9. Lorsque $p = \operatorname{car}(K)$ divise n, si on écrit $n = pm$, on a $X^p - 1 = (X-1)^p$. Ceci nous donne donc $X^n - 1 = X^{pm} - 1 = (X^m - 1)^p$ de sorte que $\mu_n(K) = \mu_m(K)$. En particulier, $\mu_n^*(K^\times) = \emptyset$.

En effet, si $\zeta \in \mu_n^*(K^\times)$, alors $\langle\zeta\rangle$ est un sous-groupe d'ordre n de $\mu_m(K^\times)$, lui-même d'ordre au plus m, ce qui est absurde.

3.3 Polynômes cyclotomiques sur $\mathbb{C}$

Comme vous l'avez certainement vu en option C, il est utile de définir les polynômes cyclotomiques aussi bien sur $\mathbb{C}$ que sur un corps fini.

Définition 3.10. Le *n-ème polynôme cyclotomique* est définit par $\Phi_n = \prod_{\zeta \in \mu_n^*(\mathbb{C})} X - \zeta$.

Proposition 3.11. *On a* $X^n - 1 = \prod_{d|n} \Phi_d$.

Démonstration. Il suffit d'observer que $\mu_n(\mathbb{C}) = \bigsqcup_{d|n} \mu_d^*(\mathbb{C})$ est l'ensemble des racines de $X^n - 1$. □

Proposition 3.12. *On a $\Phi_n \in \mathbb{Z}[X]$ et ce polynôme est unitaire.*

Démonstration. On procède par récurrence sur n. Si $n = 1$, alors $\Phi_1 = X - 1$.

Hérédité : On pose $F = \prod_{\substack{d|n \\ d \neq n}} \Phi_d \in \mathbb{Z}[X]$ par hypothèse de récurrence et on effectue la division euclidienne dans $\mathbb{Q}[X]$ de $X^n - 1$ par F. Cela donne $F\Phi_n = X^n - 1 = QF + R$ avec $\deg R < \deg F$ où on peut choisir $Q, R \in \mathbb{Z}[X]$ car F est unitaire. Donc $R = (\Phi_n - Q)\, F$. Pour des raisons de degré, on a $0 = \Phi_n - Q = R$. Donc $\Phi_n \in \mathbb{Z}[X]$. □

Remarque 3.13. En appliquant la formule d'inversion de Möbius dans le groupe abélien $\mathbb{C}(X)^\times$, on trouve directement $\Phi_n = \prod_{d|n} \left(X^{\frac{n}{d}} - 1\right)^{\mu(d)}$.

3.4 Polynômes cyclotomiques sur un corps de « bonne » caractéristique

On suppose dans cette partie que K est un corps de caractéristique p (éventuellement $p = 0$) ne divisant pas n.

On définit K_n comme étant le corps de décomposition de $X^n - 1$ sur K.

Lemme 3.14. *Soit $n \in \mathbb{N}^*$ et K un corps de caractéristique p ne divisant pas n. Alors*

1. *$X^n - 1$ est sans facteur carré dans K.*
2. *L'ensemble des racines de Φ_n dans K est $\mu_n^*(K)$.*

Démonstration.

1. Si $X^n - 1$ a un facteur carré Q, on écrit $X^n - 1 = Q^2 R$ avec $Q, R \in K[X]$. En dérivant, on a $nX^{n-1} = Q(2Q'R + QR')$ donc Q divise $X^n - 1$ et nX^{n-1}. Comme n est inversible dans K par hypothèse sur la caractéristique, on en déduit que $Q | \operatorname{pgcd}(X^n - 1, X^{n-1}) = 1$.
2. Soit $\zeta \in K$ une racine de $X^n - 1$. Comme $X^n - 1 = \prod_{d|n} \Phi_d$, la racine ζ est racine de l'un des Φ_d. Mais ζ si est une racine primitive, alors ζ n'est pas racine de Φ_d pour $d|n,\ d \neq n$, donc est racine de Φ_n. Si ζ n'est pas une racine primitive, alors il existe $e|n,\ e \neq n$ tel que $\zeta^e = 1$, donc ζ est racine de $\Phi_d | X^e - 1$ pour un certain $d|e|n,\ d \neq n$. □

Proposition 3.15. *Si* $\operatorname{car}(K) \nmid n$, *alors* $\operatorname{Card}(\mu_n(K_n)) = n$ *et* $\operatorname{Card}(\mu_n^*(K_n)) = \varphi(n)$.

En particulier, $\mu_n(K_n)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\mu_n^*(K_n)$ est l'ensemble des générateurs de ce groupe cyclique qu'on identifie à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Démonstration. Le polynôme $X^n - 1$ est sans facteur carré donc ne possède pas de racine multiple dans K_n, où il est alors scindé à racines simples. Ainsi, $\mu_n(K_n)$ est un groupe cyclique d'ordre n et les éléments de $\mu_n^*(K_n)$ sont alors exactement les éléments d'ordre n de $\mu_n(K_n)$. □

Définition 3.16. Si $p \nmid n$, on définit le n-ème polynôme cyclotomique par :

$$\Phi_{n,K} = \prod_{\zeta \in \mu_n(K_n)} (X - \zeta)$$

Exercice 6. Montrer, en utilisant des extensions de corps, qu'on peut se ramener à l'un des cas $K = \mathbb{Q}$ ou $K = \mathbb{F}_p$.

Proposition 3.17. *On suppose $p \nmid n$. Soit $\iota : \mathbb{Z} \to K$ le morphisme canonique. Alors $\Phi_{n,K} = \iota(\Phi_n)$.*

Démonstration. Remarquons d'abord que $\mu_n(K_n) = \bigsqcup_{d|n} \mu_d^*(K_n)$ car $X^n - 1$ est scindé à racines simples sur K_n. Ainsi,

$$X^n - 1 = \prod_{\zeta \in \mu_n(K_n)} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_d^*(K_n)} = \prod_{d|n} \Phi_{d,K_n}$$

On pose $\Psi_n = \iota(\Phi_n)$ et on va montrer par récurrence sur $n \in \mathbb{N}^*$ tel que $p \not| n$ que $\Psi_n = \Phi_{n,K_n}$. Si $n = 1$, alors $\Psi_n = \Phi_{n,K_n} = X - 1$.

Hérédité : On a $\prod_{d|n} \Phi_{d,K_n} = X^n - 1 = \iota\left(X^n - 1\right) = \iota\left(\prod_{d|n} \Phi_d\right) = \prod_{d|n} \Psi_d$. Les $d|n$ vérifient l'hypothèse donc par hypothèse de récurrence, on a $\Phi_{d,K_n} = \Psi_d$ pour tout $d|n$ tel que $d \neq n$. Comme l'anneau $K_n[X]$ est intègre, on a alors $\Phi_{n,K_n} = \Psi_n$. □

3.5 Facteurs irréductibles des polynômes cyclotomiques

Théorème 3.18 (Irréductibilité des polynômes cyclotomiques)**.** *Pour tout $n \in \mathbb{N}^*$, le polynôme Φ_n est irréductible sur $\mathbb{Z}$.*

Démonstration. **Étape 1 :** Comme $\mathbb{Z}[X]$ est factoriel, on peut écrire $\Phi_n = \prod_{i=1}^r Q_i$ avec $Q_i \in \mathbb{Z}[X]$ irréductible. Le produit des coefficients dominants des Q_i est 1 donc les Q_i sont tous de coefficients dominant ± 1 et le nombre de -1 est pair. Quitte à remplacer certains Q_i en $-Q_i$, on peut supposer que les Q_i sont unitaires.

Étape 2 : Soit $\zeta \in \mu_n^*(\mathbb{C})$. Pour tout nombre premier p ne divisant pas n, l'élément ζ^p dans $\mu_n(\mathbb{C}) \simeq \mathbb{Z}/n\mathbb{Z}$ est encore un générateur car de même ordre n que ζ, donc $\zeta^p \in \mu_n^*(\mathbb{C})$.

Étape 3 : Soient $i, j \in [\![1, r]\!]$ tels que $Q_i(\zeta) = 0 = Q_j(\zeta^p)$. Supposons par l'absurde qu'il est possible de choisir $i \neq j$. Considérons le morphisme de $\mathbb{Q}$-algèbres $\begin{array}{rccc} \text{év}_\zeta : & \mathbb{Q}[X] & \to & \mathbb{C} \\ & P & \mapsto & P(\zeta) \end{array}$. Son noyau est (Q_i) car Q_i est irréductible et annule ζ. En particulier $Q_j \circ X^p \in \ker \text{év}_\zeta = (Q_i)$. Par unicité de l'écriture du polynôme primitif, on en déduit que $Q_j \circ X^p = RQ_i$ pour un certain $R \in \mathbb{Z}[X]$ unitaire.

Étape 4 : Notons $\bar{\cdot} : \mathbb{Z} \to \mathbb{F}_p$ la réduction modulo p, qu'on étend canoniquement par propriété universelle en $\bar{\cdot} : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ et $F : \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ le morphisme de Frobenius, qui est un morphisme d'algèbres. Alors $\left(\overline{Q_j}\right)^p = F(\overline{Q_j}) = \overline{Q_j}(F(X)) = \overline{Q_j}(X^p) = \overline{Q_j \circ X^p} = \overline{Q_i R}$. Soit π un facteur irréductible de $\overline{Q_i}$ dans $\mathbb{F}_p[X]$, ce qui existe car $\deg(\overline{Q_i}) = \deg(Q_i) > 0$. Sur $\mathbb{F}_p$, on a $\pi | \overline{Q_i R} = \overline{Q_j}^p$. Par le lemme de Gauss, on a $\pi | \overline{Q_j}$, donc $\pi^2 | \overline{Q_i Q_j} | \overline{\Phi_n} | \overline{X^n - 1}$. On aboutit ainsi à une contradiction avec $i \neq j$ via le lemme (1.).

Étape 5 : Soit $\zeta' \in \mu_n^*(\mathbb{C})$. Comme ζ engendre $\mu_n^*(\mathbb{C})$, il existe $m \in \mathbb{N}$ tel que $\zeta' = \zeta^m$. Comme ζ' est d'ordre n et que $\zeta'^{\frac{n}{\text{pgcd}(m,n)}} = \zeta^{\frac{nm}{\text{pgcd}(m,n)}} = \zeta^{\text{ppcm}(m,n)} = 1$, on en déduit que n, l'ordre de ζ', divise $\frac{n}{\text{pgcd}(m,n)}$, donc que $\text{pgcd}(m, n) = 1$. On montre alors, par récurrence sur le nombre de facteurs irréductibles de ζ', que toute racine de Φ_n est racine de Q_i. Ainsi $\Phi_n | Q_i | \Phi_n$. Donc Q_i est le seul facteur irréductible de Φ_n. □

Corollaire 3.19. *Si $\zeta = e^{\frac{2i\pi}{n}}$, on a $\text{Dec}_{\mathbb{Q}}(X^n - 1) = \mathbb{Q}(\zeta) \simeq \mathbb{Q}[X]/(\Phi_n)$. De plus, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.*

Exercice 7. Montrer que la plus petite extension de $\mathbb{Q}$ contenant toutes les racines n-ièmes de l'unité est de degré $\varphi(n)$ sur $\mathbb{Q}$.

Les polynômes cyclotomiques donnent alors une famille de polynômes irréductibles de $\mathbb{Z}[X]$. Cependant, comme la démonstration le suggère, ces polynômes ne sont en général pas irréductibles sur un corps fini. Par exemple $\Phi_8 = X^4 - X^2 + 1 = \left(X^2 + X + 1\right)$ sur $\mathbb{F}_2$. et on a le résultat suivant :

Théorème 3.20. *Soit $\kappa = \mathbb{F}_q$ un corps fini à q éléments et $n \in \mathbb{N}^*$ un entier premier à q. Soit r l'ordre de $\overline{q} \in \mathbb{Z}/n\mathbb{Z}$. Alors les facteurs irréductibles de Φ_n dans $\mathbb{F}_q$ sont deux à deux distincts et de degré r.*

Démonstration. Soit P un facteur irréductible de Φ_n de degré s et $K = \mathbb{F}_q[X]/(P)$, corps de rupture de P sur $\mathbb{F}_q$, qui est donc un corps fini de cardinal q^s. Par construction, K contient une racine de Φ_n, disons $\zeta \neq 0$ qui est donc une racine primitive n-ième de l'unité par le lemme (2.), donc d'ordre n. On a $\zeta^{q^s} = \zeta$ donc $n | q^s - 1$. Ainsi $q^s \equiv 1 \mod n$ et donc $s \geq r$.

Inversement, comme $\zeta^n = 1$ et $q^r \equiv 1 \mod n$, on a $\zeta^{q^r} = \zeta$. Soit L le sous-corps de K formé des racines de $X^{q^r} - X$. Alors $\zeta \in L$ mais $K = \mathbb{F}_q[\zeta]$ par construction comme corps de rupture, donc $L = K = \mathbb{F}_q[\zeta]$. Donc $q^s = \text{Card}(K) \leq q^r$ et ainsi $r \geq s$ car $q \geq 2$.

Ainsi, tous les facteurs irréductibles de Φ_n sont de degré r. De plus, ils sont deux à deux distincts car $\Phi_n | X^n - 1$ qui est sans facteur carré sur $\mathbb{F}_q$ par le lemme. □

Corollaire 3.21. *Le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{F}_q$ si, et seulement si, $\overline{q} \in \mathbb{Z}/n\mathbb{Z}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. Φ_n est irréductible si, et seulement si, l'ordre de $\overline{q}$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est $r = \deg(\Phi_n) = \varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$. □

En particulier, les Φ_{2^m} ne sont jamais irréductibles sur $\mathbb{F}_q$, sauf si $m \in \{1, 2\}$.

3.6 Application aux calculs dans les corps finis

On a vu que $\mathbb{F}_q^\times$ est cyclique. En particulier, si α est un générateur de $\mathbb{F}_q^\times$, alors $\mathbb{F}_q = \mathbb{F}_p[\alpha]$ (résultat qu'on peut qualifier de théorème de l'élément primitif dans les corps finis).

L'intérêt d'un tel générateur est que, une fois déterminé, on dispose d'une représentation des éléments le corps $\mathbb{F}_q$ qui est favorable à faire des multiplications, ce qui est souvent coûteux usuellement. En effet, tout élément de $\mathbb{F}_q^\times$ s'écrit α^m pour un $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Ensuite, si on veut en plus faire des additions, il s'agit de trouver un polynôme annulateur de α, de sorte que $(1, \alpha, \ldots, \alpha^{r-1}$ soit une $\mathbb{F}_p$-base de $\mathbb{F}_q$. Or on sait que α est une racine primitive $q-1$-ème de l'unité, donc racine du polynôme cyclotomoque Φ_{q-1}.

Corollaire 3.22. *Dans l'anneau $\mathbb{F}_p[X]$, les facteurs irréductibles de Φ_{p^r-1} sont de degré r.*

Un tel facteur est appelé un *polynôme primitif* sur $\mathbb{F}_p$ et ses racines sont des racines primitives $p^r - 1$-ièmes de 1. En particulier, $\mathbb{F}_{p^r} = \mathbb{F}_p[\zeta]$ pour ζ un générateur de $\mathbb{F}_{p^r}^\times$.

Exemple 3.23. Pour construire $\mathbb{F}_{16}$, on doit choisir un facteur irréductible de $\Phi_{15} = \frac{X^{15}-1}{\Phi_1\Phi_3\Phi_5}$. On trouve $\Phi_{15} = \left(X^4 + X^3 + 1\right)\left(X^4 + X + 1\right)$. Ainsi $\mathbb{F}_{16} = \mathbb{F}_2[X]/\left(X^4 + X + 1\right) = \mathbb{F}_2[\alpha]$ et l'élément α vérifiant $\alpha^4 = \alpha + 1$ est un générateur de $\mathbb{F}_{16}^\times$.

Ainsi $\mathbb{F}_{16} = \left\{1, \alpha, \alpha^2, \ldots, \alpha^{15}\right\}$ et la table de multiplication est immédiate. La table d'addition se dresse ensuite facilement en exploitant la relation $\alpha^4 = \alpha + 1$. Par exemple $\alpha^5 = \alpha^2 + \alpha$ et $\alpha^8 = \alpha^2 + 1$ donc $\alpha^5 + \alpha^8 = \alpha + 1 = \alpha^4$.

3.7 Une remarque culturelle sur certains groupes linéaires sur un corps

Soit K un corps.

On dispose d'une injection naturelle $j : \mathrm{SL}_n(K) \hookrightarrow \mathrm{GL}_n(K)$ et d'un morphisme de groupes quotient $\mathrm{GL}_n(K) \twoheadrightarrow \mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/K^\times I_n$. On peut alors considérer le morphisme de groupes $f = \pi \circ j : \mathrm{SL}_n(K) \to \mathrm{PGL}_n(K)$.

Tout d'abord on observe que $\ker f = j^{-1}(K^\times I_n) = K^\times I_n \cap \mathrm{SL}_n(K) = \mu_n(K) I_n$. On dispose alors d'une première suite exacte :

$$1 \to \mu_n(K) \to \mathrm{SL}_n(K) \xrightarrow{f} \mathrm{PGL}_n(K)$$

D'un autre côté, on dispose d'un morphisme de groupes induit par le déterminant : $\det : \mathrm{GL}_n(K) \to K^\times$. On observe que l'image par ce morphisme du centre de $\mathrm{GL}_n(K)$ est $\det(K^\times I_n) \subset K^{\times n}$ l'ensemble des puissances n-èmes dans $K^\times$. En considérant le morphisme de groupes quotient $q : K^\times \twoheadrightarrow K^\times/K^{\times n}$, on peut alors définir un morphisme de groupes $q \circ \det : \mathrm{GL}_n(K) \to K^\times/K^{\times n}$ qui est surjectif par composition. Comme $K^\times I_n \subset \ker q$, celui-ci induit alors un morphisme de groupes $\delta : \mathrm{PGL}_n(K) \to K^\times/K^{\times n}$ qui est encore surjectif.

Enfin, on peut vérifier que $\mathrm{im}(f) = \ker \delta$ de sorte qu'on a en fait une suite exacte de groupes :

$$1 \to \mu_n(K) \to \mathrm{SL}_n(K) \xrightarrow{f} \mathrm{PGL}_n(K) \xrightarrow{\delta} K^\times/K^{\times n} \to 1$$

Lorsque n est une puissance de $\mathrm{car}(K) = p$, on sait alors que $\mu_n(K) = 1$. On observe dans ce cas que $\mathrm{SL}_n(K)$ s'identifie à un sous-groupe distingué de $\mathrm{PGL}_n(K)$ et que $K^\times/K^{\times n}$ s'identifie au quotient $\mathrm{PGL}_n(K)/\mathrm{SL}_n(K)$.

4 Polynômes à n indéterminées

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

4.1 Algèbre sur un anneau

Définition 4.1. Une A-algèbre B (associative et unifère) est la donnée d'un anneau B et d'un morphisme d'anneau $\rho : A \to \mathcal{Z}(B)$ où $\mathcal{Z}(B) = \{z \in B,\ \forall b \in B,\ zb = bz\}$.

Remarque 4.2. On peut donner d'autres définitions plus générales lorsqu'on ne suppose pas B unifère, ou associative, mais je n'en vois pas l'intérêt dans le cadre de l'agrégation.

Le morphisme ρ n'est en général pas injectif. Il permet de munir B d'une structure naturelle de A-module via $a \cdot b = \rho(a)b$.

Exemple 4.3. Un anneau est une $\mathbb{Z}$-algèbre pour le morphisme canonique $\mathbb{Z} \to A$ qui envoie $n \mapsto n\mathbf{1}_A$.

L'anneau $\mathcal{M}_n(A)$ est un exemple de A-algèbre non-commutative pour le morphisme naturel $f : x \mapsto xI_n$.

Avant toute chose, rappelons brièvement la propriété universelle des algèbres de polynômes :

Théorème 4.4 (Propriété universelle des algèbres de polynômes (finies))**.** *Soit A un anneau commutatif et B une A-algèbre. Soit $n \in \mathbb{N}^*$. Soient $\mathbf{b} = (b_1, \dots, b_n)$ un n-uplet d'éléments de B qui commutent deux à deux. Alors il existe un unique morphisme de A-algèbres $\varphi = \mathrm{ev}_{\mathbf{b}} : A[X_1, \dots, X_n] \to B$ tel que $\varphi(X_i) = b_i$ pour tout $i \in [\![1, n]\!]$.*

Ceci définit en particulier $P(\mathbf{b}) = \varphi(P)$ et permet de manipuler des formules usuelles. On notera que la condition de commutativité est vide si $n = 1$, ce qui est le cas en général quand on manipule des polynômes d'endomorphisme en algèbre linéaire par exemple.

Corollaire 4.5. *On a un isomorphisme d'algèbres naturel $A[X_1, \dots, X_n][Y] \simeq A[X_1, \dots, X_n, Y]$.*

Corollaire 4.6. *À tout polynôme $P \in A[X_1, \dots, X_n]$, on associe une fonction $f_P : A^n \to A$ dite polynômiale, donnée par $(x_0, \dots, x_n) \mapsto P(x_0, \dots, x_n) = \mathrm{ev}_{x_1,\dots,x_n}(P)$.*

Remarque 4.7. Si B est une R-algèbre et $\rho : A \to R$ est un morphisme d'anneau, alors B hérite d'une structure de A algèbre via ρ mais il faudra alors remarquer que les coefficients de P via φ sont « modifiés » par ρ.

On se fixe un entier naturel $n \in \mathbb{N}^*$ et on considère l'algèbre $A[X_1, \dots, X_n]$ des polynômes à n indéterminées sur un anneau A.

4.2 Degré, polynômes homogènes

Notation 4.8. Pour tout n-uplet d'entiers naturels $\mathbf{m} = (m_1, \dots, m_n)$ on notera $X^{\mathbf{m}} = X_1^{m_1} \cdots X_n^{m_n}$.

Définition 4.9. Un *monôme* est un polynôme de la forme $aX^{\mathbf{m}} = aX_1^{m_1} \cdots X_n^{m_n}$ avec $a \in A$ et $(m_1, \dots, m_n) \in \mathbb{N}^n$. Il est *non nul* si $a_{\mathbf{m}} \neq 0$.

Son *degré total*, ou plus simplement son *degré*, est $\deg(aX_1^{m_1} \cdots X_n^{m_n}) = \begin{cases} -\infty & \text{si } a = 0 \\ \sum_{i=1}^n m_i & \text{sinon.} \end{cases}$

Son *multidegré* est $\mathrm{mdeg}\,(X_1^{m_1} \cdots X_n^{m_n}) = (m_1, \dots, m_n)$.

Le *degré total* (ou *degré*) d'un polynôme $P = \sum_{\mathbf{m}=(m_1,\dots,m_n)\in\mathbb{N}^n} a_{\mathbf{m}} X_1^{m_1} \cdots X_n^{m_n}$ est le maximum des degrés des monômes qui le constituent, autrement dit, $\deg(P) = \begin{cases} -\infty & \text{si } P = 0 \\ \max\{\sum_{i=1}^n,\ a_{\mathbf{m}} \neq 0\} & \text{sinon.} \end{cases}$.

Le *degré partiel* en X_i d'un polynôme $P \in A[X_1, \dots, X_n]$, noté $\deg_{X_i}(P)$, est le degré du polynôme canoniquement associé à P dans l'anneau $A[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i]$.

Fait 4.10. *Pour tous $P, Q \in A[X_1, \dots, X_n]$, on a :*
(1) $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ *avec égalité si* $\deg(P) \neq \deg(Q)$ *;*
(2) $\deg(PQ) \leq \deg(P) + \deg(Q)$ *avec égalité si A est intègre.*

Définition 4.11. Un polynôme est dit *homogène* de degré d si les monômes non nuls qui le constituent sont tous de degré d.

Une *forme algébrique* de degré d à n variables est l'application polynomiale $f_P : K^n \to K$ associée à un polynôme $P \in K[X_1, \dots, X_n]$ homogène de degré d.

Exemple 4.12.

(1) Une forme algébrique de degré 1 est une forme linéaire.

(2) Une forme algébrique de degré 2 est une forme quadratique.

(n) Le déterminant $\det = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} X_{\sigma(j),j}$ est un polynôme homogène en n^2 variables de degré n. La forme algébrique associée $f_{\det}$ de degré n permet de définir une application n-linéaire alternée f sur le A-module libre A^n, donnée par $f\left(\sum x_{1j}, \dots, \sum x_{nj}\right) = f_{\det}(x_{i,j})$.

Fait 4.13. *L'ensemble des polynômes homogènes de degré d est un A-module libre de rang $\binom{n+d-1}{d}$ et de base $\left(X_1^{m_1} \cdots X_n^{m_n}\right)_{\mathbf{m}}$ où $\mathbf{m} = (m_1, \dots, m_n) \in \mathbb{N}^n$ vérifie $m_1 + \cdots + m_n = d$.*

Exemple 4.14.

(1) L'espace vectoriel des formes linéaires sur K^n est de dimension n.

(2) L'espace vectoriel des formes quadratiques sur K^n est de dimension $\binom{n+2-1}{n} = \frac{n(n+1)}{2}$.

Voici deux liens entre les polynômes à plusieurs variables et les polynômes homogènes :

Lemme 4.15. *Soit $P \in A[X_1, \dots, X_n]$ un polynôme, $Q(T) = P(TX_1, \dots, TX_n) \in A[X_1, \dots, X_n][T]$ et $d \in \mathbb{N}$. S'équivalent :*

(i) le polynôme $P \in A[X_1, \dots, X_n]$ est homogène de degré d ;

(ii) $Q(T) = T^d P(X_1, \dots, X_n)$;

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

Démonstration. Soit $P = \sum_{\mathbf{m}} a_{\mathbf{m}} X^{\mathbf{m}} \in A[X_1, \dots, X_n]$. Alors $Q(T) = \sum_{d \in \mathbb{N}} \sum_{\substack{\mathbf{m} \in \mathbb{N}^n \\ m_1 + \cdots + m_n = d}} a_{\mathbf{m}} X^{\mathbf{m}} T^d$. $(i) \Rightarrow (ii)$ car tous les monômes non nuls ont degré d donc on peut ôter la somme sur $d \in \mathbb{N}$. $(ii) \Rightarrow (iii)$ est évident. $(iii) \Rightarrow (i)$ car tout monôme de P doit être soit nul, soit de degré d. □

Proposition 4.16 (Échelonnement en degré)**.** *Tout polynôme $P \in A[X_1, \dots, X_n]$ s'écrit de manière unique sous la forme $P = \sum_{d \in \mathbb{N}} P_d$ avec $P_d \in A[X_1, \dots, X_n]$ homogène de degré d.*

Démonstration. **Existence :** Soit $Q(T) = P(TX_1, \dots, TX_n) \in A[X_1, \dots, X_n][T]$. On écrit alors $Q(T) = \sum_{d \in \mathbb{N}} P_d T^d$ avec $P_d = \sum_{\substack{\mathbf{m} \in \mathbb{N}^n \\ m_1 + \cdots + m_n = d}} a_{\mathbf{m}} X^{\mathbf{m}}$. Les P_d sont homogènes de degré d par construction.

Unicité : Si $P = \sum_{d \in \mathbb{N}} P'_d$ avec P'_d homogène de degré d. Alors $Q(T) - Q(T) = 0 = \sum_{d \in \mathbb{N}} P'_d(TX_1, \dots, TX_n) - P(TX_1, \dots, TX_n) = \sum_{d \in \mathbb{N}} T^d (P'_d - P_d)$. Donc $P'_d = P_d$. □

Définition 4.17. Si $P \in A[X_1, \dots, X_n]$, on appelle *homogénéisé* de P le polynôme homogène :

$$X_0^d P\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right) \in A[X_0, \dots, X_n] \quad \text{où} \quad d = \deg(P).$$

Voici quelques propriétés des polynômes homogènes, laissées en exercice au lecteur :

Proposition 4.18.
1. *Si $P \in K[X_0, \dots, X_n]$ est homogène, alors l'application polynomiale f_P est homogène, c'est-à-dire que $f_P(\lambda x) = \lambda^{\deg(P)} f_P(x)$.*
2. *Réciproquement si K est infini et f_P est homogène, alors P est homogène.*
3. *Les facteurs irréductibles d'un polynôme homogène sont homogènes de degré inférieur.*

Remarque 4.19. Il existe un lien fort entre les lieux de zéros de polynômes et la géométrie. Par exemple, X^2+Y^2-1 définit un polynôme dans $\mathbb{R}[X, Y]$ dont le lieu des zéros dans $\mathbb{R}$ est un cercle. Plus généralement, une *conique* dans K^2 est, par définition, le lieu d'annulation d'un polynôme de $K[X, Y]$ de degré total 2 ; une *quadrique* dans K^3 est le lieu d'annulation d'un polynôme de $K[X, Y, Z]$ de degré total 2.

Pour un polynôme homogène $P \in K[X_1, \dots, X_n]$, on dispose d'une forme algébrique $f_P : K^n \to K$ qui est une fonction homogène. En particulier, étant donné une droite vectoriel D de K^n, on a la disjonction suivante :

— soit f_P s'annule sur D ;

— soit f_P ne s'annule pas sur $D \setminus \{0\}$.

On ne peut pas définir directement de fonction polynômiale sur l'espace projectif (i.e. l'espace des droites vectorielles), mais on peut donner un sens à l'équation $P[x_0 : \ldots : x_n] = 0$.

Par exemple, le polynôme $X^2 + Y^2 - Z^2$, qui est l'homogénéisé de $X^2 + Y^2 - 1$ définit un cône de $\mathbb{R}^3$ et, en fait, une conique dans $\mathbb{P}^2(\mathbb{R})$. Une conique projective est alors, par définition, le lieu d'annulation dans $\mathbb{P}^2(K)$ d'un polynôme homogène de degré 2 de $K[X, Y, Z]$.

On étudiera plus en détails ces propriétés géométriques dans le cours de géométrie et dans le prochain cours sur les formes quadratiques, ainsi que quelques éléments de classifications.

4.3 Polynômes symétriques

Considérons le groupe $G = \mathfrak{S}_n$ et B la A-algèbre $A[X_1, \ldots, X_n]$ des polynômes à n indéterminées. La propriété universelle donne l'existence d'un unique automorphisme de A-algèbres $\varphi_\sigma : B \to B$ tel que $X_i \mapsto X_{\sigma(i)}$. On note P^σ le polynôme $\varphi_\sigma(P) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.

Ceci définit une action de groupes $\mathfrak{S}_n \circlearrowleft A[X_1, \ldots, X_n]$.

Définition 4.20. Un polynôme $P \in A[X_1, \ldots, X_n]$ est dit *symétrique* s'il est fixé par l'action de $\mathfrak{S}_n$. Le polynôme symétrique $\Sigma_k^n = \sum_{1 \leq i_1 < \cdots < i_k \leq n} \prod_{j=1}^{k} X_{i_j}$ est appelé *k-ième polynôme symétrique élémentaire.*

Par convention, on posera $\Sigma_0^n = 1$.

Exemple 4.21. $\Sigma_1^n = X_1 + \cdots + X_n$ et $\Sigma_n^n = X_1 \cdots X_n$.

Exercice 8. Écrire Σ_2^4 et Σ_3^4. Combien de monômes non nuls constituent le polynôme Σ_k^n ?

Théorème 4.22. *L'ensemble $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ des polynômes symétriques est une sous-A-algèbre de $A[X_1, \ldots, X_n]$ engendrée par les Σ_k^n.*

Démonstration. La preuve de ce théorème est fondamentale car elle fournit également un algorithme qui permet d'écrire explicitement un polynôme symétrique comme polynôme en les polynômes symétriques élémentaires. On considère l'ordre lexicographique, noté $\succ$, sur $\mathbb{N}^n$ donné par

$$\mathbf{a} = (a_1, \ldots, a_n) \succ \mathbf{b} = (b_1, \ldots, b_n) \iff \exists k \in [\![0, n-1]\!],\ a_{k+1} > b_{k+1} \text{ et } \forall i \leq k,\ a_i = b_i$$

Pour $P = \sum_{\mathbf{m} \in \mathbb{N}^n} a_{\mathbf{m}} X^{\mathbf{m}}$, on définit son multidegré par $\mathrm{mdeg}(P) = \max\{\mathbf{m} \in \mathbb{N}^n,\ a_{\mathbf{m}} \neq 0\}$ où le maximum est pris pour l'ordre lexicographique $\succ$. On dira que $a_{\mathrm{mdeg}(P)}$ est le coefficient dominant de P.

Soit P un polynôme symétrique de multidegré $\mathbf{m} = (m_1, \ldots, m_n)$. On cherche alors un polynôme $Q \in A[\Sigma_1^n, \ldots, \Sigma_n^n] \subset A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ ayant même coefficient dominant que P et même multidegré.

Lemme 4.23. *Si P est symétrique de multidegré $\mathbf{m}$, alors $m_1 \geq m_2 \geq \cdots \geq m_n$.*

Démonstration. Soit $\sigma \in \mathfrak{S}_n$. Notons $\mathbf{m}^\sigma = \left(m_{\sigma(1)}, \ldots, m_{\sigma(n)}\right)$. Le monôme $\sigma \cdot X^{\mathbf{m}} = X^{\mathbf{m}^\sigma}$ apparait dans $P^\sigma = P$. Comme $\mathbf{m} \succ \mathbf{m}^\sigma$, on a $m_1 \geq m_{\sigma(1)}$. Ceci étant valable pour tout $\sigma \in \mathfrak{S}_n$, il vient $\alpha_1 \geq \alpha_i$ pour tout i. Plus généralement, pour tout $k \in [\![1, n-1]\!]$, on montre que $m_k \geq m_{\sigma(k)}$ pour tout σ tel que $\sigma_{|[\![1,k-1]\!]} = \mathrm{id}_{[\![1,k-1]\!]}$. Ainsi, on a bien $m_1 \geq m_2 \geq \cdots \geq m_n$. □

On peut donc définir $Q = (\Sigma_1^n)^{m_1 - m_2} \cdots \left(\Sigma_{n-1}^n\right)^{m_{n-1} - m_n} (\Sigma_n^n)^{m_n} \in A[\Sigma_1^n, \ldots, \Sigma_n^n]$. On a :

$$\mathrm{mdeg}(Q) = \sum_{i=1} (m_i - m_{i+1}) \,\mathrm{mdeg}\left(\Sigma_i^n\right)$$

avec $m_{n+1} = 0$. Or $\mathrm{mdeg}\left(\Sigma_i^n\right) = \mathrm{mdeg}\left(X_1 \cdots X_i\right) = (\underbrace{1, \ldots, 1}_{i \text{ termes}}, 0, \ldots, 0)$. D'où :

$$\mathrm{mdeg}(Q) = (m_1 - m_2, 0, \ldots, 0) + (m_2 - m_3, m_2 - m_3, 0, \ldots, 0) + \cdots + (m_n, \ldots, m_n) = \mathbf{m}.$$

Soit $\widetilde{P} = P - a_{\mathbf{m}} Q$. Alors $\mathrm{mdeg}(P) \succ \mathrm{mdeg}(\widetilde{P})$. Comme $\succ$ est un bon ordre sur $\mathbb{N}^n$, on en déduit que la suite définie par $P_0 = P$ et $P_{i+1} = \widetilde{P_i}$ stationne en 0 et, en particulier, que $P \in A[\Sigma_1^n, \ldots, \Sigma_n^n]$ car $P = \sum P_i - P_{i+1}$ avec $P_i - P_{i+1} = P_i - \widetilde{P_i} \in A[\Sigma_1^n, \ldots, \Sigma_n^n]$. □

Exercice 9. Montrer que $P = X_1^3 + X_2^3 + X_3^3$ est symétrique et l'écrire comme un polynôme en les polynômes symétriques élémentaires.

Puisqu'on s'intéresse à l'action du groupe $\mathfrak{S}_n$, il est naturel de s'intéresser également à l'action du sous-groupe $\mathfrak{A}_n$. On note $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ la signature. Parce qu'on a besoin de distinguer 1 et -1, on suppose que A est un anneau intègre de caractéristique $\mathrm{car}(A) \neq 2$. On est d'abord amené à introduire la notion suivante :

Définition 4.24. Un polynôme $P \in K[X_1, \ldots, X_n]$ est dit *antisymétrique* si pour tout $\sigma \in \mathfrak{S}_n$, on a $\sigma \cdot P = \varepsilon(\sigma)P$.

Exemple 4.25. Le polynôme $\Delta = \prod_{1 \leq i < j \leq n}(X_i - X_j)$ est antisymétrique. En fait, c'est un polynôme antisymétrique non nul de degré minimal et il engendre le module des polynômes antisymétriques sur l'anneau des polynômes symétriques.

Voici quelques propriétés laissées en exercices :

Proposition 4.26.
(1) Pour tout polynôme antisymétrique Q, il existe un unique polynôme symétrique P tel que $Q = \Delta P$.
(2) Les polynômes $P \in A[X_1, \ldots, X_n]$ fixés par l'action de $\mathfrak{A}_n$ sont exactement ceux qui s'écrivent sous la forme $P = S + \Delta T$ avec S, T symétriques. De plus, une telle écriture est unique.

4.4 Relations coefficients-racines

Dans la suite, on suppose que l'anneau A est intègre.

Définition 4.27. Soit $P \in A[T]$ un polynôme en une indéterminée. On dit que a est une racine d'ordre m si $(X-a)^m | P$ et $(X-a)^{m+1} \not| P$.

Exemple 4.28. Un élément $\alpha \in A$ est racine d'ordre supérieur à 2 si, et seulement si, $P(\alpha) = 0 = P'(\alpha)$. En revanche, on n'a pas de résultat analogue pour un ordre $m \geq 3$. Par exemple, si A est intègre de caractéristique 2, alors $P = X^2$ vérifie $P^{(k)}(0) = 0$ pour tout k mais 0 n'est pas racine d'ordre 3 car X^3 ne divise pas P.

Exercice 10. Soit A un anneau commutatif intègre et $n \in \mathbb{N}^*$.

1. Soient $P \in A[X]$ et $a_1, \ldots, a_n$ des éléments de A deux à deux distincts. Soit $(m_1, \ldots, m_n) \in \mathbb{N}^n$.
   (a) Montrer que s'équivalent :
      (i) pour tout $i \in [\![1, n]\!]$, l'élément a_i est racine d'ordre supérieur à m_i de P ;
      (ii) le polynôme $\prod_{i=1}^n (X - a_i)^{m_i}$ divise P.
      Indication : on pourra se ramener à l'anneau euclidien $\mathrm{Frac}(A)[X]$.
   (b) En déduire que sous ces conditions $\deg(P) \geq \sum_{i=1}^n m_i$.
2. Soit $P \in A[X_1, \ldots, X_n]$.
   (a) Soient $E_1, \ldots, E_n$ des parties infinies de A. Montrer que f_P est nulle sur $E_1 \times \cdots \times E_n$ si, et seulement si, $P = 0$.
   (b) Montrer que si $A = \mathbb{R}$ et f_P est nulle sur un ouvert Ω de $\mathbb{R}^n$, alors $P = 0$.

Lemme 4.29. *Soit A un anneau commutatif. Dans $A[X_1, \ldots, X_d][T]$, on a l'égalité :*

$$\prod_{i=1}^{d} (T - X_i) = \sum_{i=0}^{d} (-1)^i \Sigma_i^d T^{d-i}.$$

Démonstration. C'est un calcul qui se fait par récurrence sur d. □

Proposition 4.30 (Relations coefficients-racines)**.** *Soit A un anneau commutatif, $\lambda \in A^\times$ et $P = \lambda \prod_{i=1}^d (X - \alpha_i) \in A[X]$ un polynôme scindé de racines $\alpha_1, \ldots, \alpha_d \in A$ comptées avec multiplicité. On écrit $P = \sum_{i=0}^d a_i X^i$. Alors $a_d = \lambda \in A^\times$ et pour tout $i \in [\![0, d-1]\!]$, on a :*

$$a_i = a_d (-1)^{d-i} \Sigma_{d-i}^d (\alpha_1, \ldots, \alpha_n).$$

Démonstration. On évalue par la propriété universelle la formule du lemme en $(\alpha_1, \ldots, \alpha_n)$, ce qui donne :

$$\lambda \prod_{i=1}^{d} (X - \alpha_i) = \sum_{i=0}^{d} \lambda (-1)^i \Sigma_i^d(\alpha_1, \ldots, \alpha_n) X^{d-i} = P.$$

□

Corollaire 4.31. *Soit A est un anneau commutatif intègre et $P = X^d + \sum_{i=0}^{d-1} a_i X^i \in A[X]$ un polynôme unitaire de degré d. Soit $K = \mathrm{Frac}(A)$ et $L = \mathrm{Dec}_K(P)$ le corps de décomposition de P sur K. Soient $\alpha_1, \ldots, \alpha_d$ les racines de P dans L comptées avec multiplicité. Alors pour tout polynôme symétrique $Q \in A[X_1, \ldots, X_n]$, il existe (un unique) polynôme $R \in A[Y_1, \ldots, Y_d]$ tel que $Q(\alpha_1, \ldots, \alpha_d) = R(a_0, \ldots, a_{d-1})$.*

En particulier, toute relation symétriques en les racines d'un polynôme est un élément de l'anneau qui contient les coefficients de ce polynôme.

Exemple 4.32. Pour tout $n \in \mathbb{N}$, on a $j^n + j^{2n} \in \mathbb{Z}$, où $j = e^{\frac{i2\pi}{3}}$.

De même, $\left(\frac{1-\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^n \in \mathbb{Z}$.