ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Révisions sur les anneaux et leurs idéaux

Leçons directement concernées (2019)

(120) Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
(122*) Anneaux principaux. Applications.
(142*) PGCD et PPCM, algorithmes de calcul. Applications.

Leçons liées, dans lesquelles on peut parler d'anneaux et idéaux (2019)

(102)* Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.
(110)* Structure et dualité des groupes abéliens finis. Applications.
(121) Nombres premiers. 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.

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.

(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.

Bibliographie

- À suivre...

1 Vocabulaire général des anneaux

Définition 1.1. A est un anneau commutatif

1.1 Notions de base

Définition 1.2. 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.

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 $a = bc$. On notera que pour tout $a \in A$, on a $1|a|0$. La relation binaire $\cdot|\cdot$ est une relation d'ordre partielle sur $A/A^\times$ pour laquelle 1 est un plus petit élément et 0 est le plus grand élément.
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 et A n'admet pas de diviseurs de 0.
Si A est intègre, alors 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 $2 \cdot 3 = \left(1 - i\sqrt{5}\right)\left(1 + i\sqrt{5}\right)$.

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

Soit A un anneau commutatif.

Définition 1.9. 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 $a \cdot i \in I$.

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

Si I et J sont des idéaux, alors $I+J = \{i+j,\ i \in I,\ j \in J\}$ est l'idéal de A engendré par I et J. On dit que I et J sont *premiers entre eux* si $I+J=A$. On note également $I \cdot J$ l'idéal engendré par la famille $(i \cdot j)_{i\in I,\ j\in J}$.

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.

Fait 1.10. *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 1.11. 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 1.12. 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 1.13. *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 1.14. 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 1.15. *Un anneau est intègre (resp. un corps) si, et seulement si,* 0 *est premier (resp. maximal).*

Théorème 1.16 (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. □

Théorème 1.17 (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. Supposons que $n=2$. 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 $\Phi(aj+bi) = (a(1-i)+bi \mod I, aj+b(1-j) \mod J) = (a \mod I, b \mod J)$. 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 $y = \underbrace{iy}_{\in IJ} + \underbrace{yj}_{\in IJ}$ et la réciproque est immédiate.

Hérédité : Supposons $n \geq 3$. Remarquons d'abord que pour tout $k \in [\![1, n-1]\!]$, on a $I_1 \cdots I_k + I_n = A$. Cela se vérifie par une récurrence immédiate car c'est vrai si $k=1$ et $A = A \cdot A = (I_1 \cdots I_{k-1} + I_n) \cdot (I_k + I_n) \subseteq I_1 \cdots I_k + I_n$. En particulier, $I_1 \cdots I_{n-1}$ et I_n sont premiers entre eux donc, par hypothèse de récurrence, on a $A/I_1 \cdots I_n \simeq A/I_1 \cdots I_{n-1} \times A/I_n \simeq A/I_1 \times \cdots \times A/I_{n-1} \times A/I_n$. □

1.3 Anneaux euclidiens et principaux

Définition 1.18. 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 1.19. 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 1.20. 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 1.21. 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 1.22 (Identités de Bézout)**.** *Soit $(a_i)_{i\in[\![1,n]\!]}$ une famille* **finie** *d'éléments de A premiers entre eux. Alors il existe des éléments u_i de A tels que $1 = u_1a_1 + \dots u_na_n$.*

Démonstration. $1 \in (a_1) + \dots + (a_n)$. □

Théorème 1.23. *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 1.24 (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 1.25 (Diviseurs élémentaires)**.** *Si A est un anneau principal et si $M \in \mathcal{M}_{r,s}(A)$, alors il existe des entiers $d_1|\dots|d_n$, 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 1.26. Dans le cas d'un anneau Euclidien, on a un algorithme explicite de calcul.

Corollaire 1.27 (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 $d_1|\dots|d_s$, uniquement déterminés, tels que $G \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \mathbb{Z}/d_s\mathbb{Z}$.*

Démonstration. La version « anneaux » de ce résultat consiste surjecter un $\mathbb{Z}$-module libre de type fini sur le groupe G. Plus précisément, si $X = \{x_1, \dots, x_n\}$ 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 $\mathcal{B} = (b_1, \dots, b_n)$ de M et des entiers $d_1 | \dots | d_n$ 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 $M/N \simeq \mathbb{Z}/d_i\mathbb{Z} \simeq G$. □

On verra plus tard une (autre) preuve utilisant uniquement des résultats de théorie des groupes dans le cas des groupes abéliens finis.

1.4 Anneaux factoriels

On définit tout d'abord deux propriétés remarquables que satisfont, entre autres, les anneaux principaux.

Définition 1.28. Soit A un anneau. On définit deux propriétés :

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

(U) $\forall u, v \in A^\times,\ \forall r, s \in \mathbb{N},\ \forall p_1, \dots, p_r, q_1, \dots, q_s \in A$ irréductibles,
on a $u p_1 \dots p_r = v q_1 \dots q_s \quad \Rightarrow \quad r = s$ 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 1.29. *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 $d = \text{pgcd}(a, b)$ 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 1.30. *Tout anneau principal est factoriel.*

Esquisse de preuve. Pour (E), on procède par l'absurde en supposant qu'on peut trouver $a \in A$ tel que a n'admet pas de telle décomposition. On construit alors une suite d'éléments $a_k \notin A^\times$ tels que pour tout $l \in \mathbb{N}$, on a $a = a_1 \cdots a_l$ et $a_{l+1} | a_l$. Cela nous donne une suite croissante d'idéaux (a_k) dont la réunion est un idéal principal (b) de A car A est principal. Nécessairement $b \in (a_k)$ pour un certain k donc la suite est stationnaire, aux inversibles près, ce qui est exclu.

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

Démonstration. Conséquence immédiate de (U). □

Exemple 1.32. 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 1.33 (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 le note $v_p(a)$ et on appelle cette quantité la *valuation p-adique de 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 :

- $\text{pgcd}(a_1, \dots, a_n)) = \prod_{p \in \mathcal{P}} p^{\min v_p(a_1), \dots, v_p(a_n)}$;
- $\text{pgcd}(a_1, \dots, a_n) = \prod_{p \in \mathcal{P}} p^{\max v_p(a_1), \dots, v_p(a_n)}$.

Fait 1.34. *Ce sont des opérations associatives (on peut parenthéser comme bon nous semble).*

Notation 1.35. 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 1.36 (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 1.37 (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 1.38. 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 1.39. *Tout anneau principal est noethérien.*
Un quotient d'un anneau noethérien est noethérien.

Exemple 1.40. L'anneau $K[X_1, \dots, X_n, \dots]$ est intègre mais n'est pas noethérien.

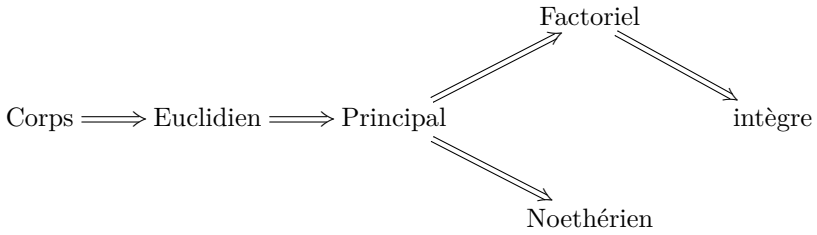
Proposition 1.41. *Si A est un anneau intègre et noethérien, alors il vérifie (E).*

Théorème 1.42 (Hilbert)**.** *Si A est noethérien, alors $A[X]$ est noethérien, donc $A[X_1, \dots, X_n]$ aussi.*

Exemple 1.43. 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.
- 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 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. Notons $\mathcal{P} \subset \mathbb{N}$ l'ensemble des nombres premiers de $\mathbb{Z}$.

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 $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

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 2.1 (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 2.2 (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 2.3. *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 : $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \left\{\overline{\pm 1}\right\} \times U(\alpha)$.*

Polynômes cyclotomiques

On va conclure ce cours en parlant d'une famille particulière de polynômes qui sera très utile pour travailler explicitement dans les corps finis.

Racines de l'unité Une autre application des formules sur l'indicatrice d'Euler est la suivante :

Définition 2.4. On note $\mu_n(K) = \{\zeta \in K,\ \zeta^n = 1\}$ le *groupe des racines n-èmes de l'unité* dans K.

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.

Théorème 2.5. *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 polynômes $P = X^d - 1$ 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 2.6. *Le groupe $\mu_n(K)$ des racines n-èmes de l'unité est cyclique.*

Remarque 2.7. Ce groupe n'est en général pas isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Par exemple, lorsque $p = \mathrm{car}(K)|n$, on a $X^p - 1 = (X-1)^p$ donc $X^n - 1 = X^{pm} - 1 = (X^m - 1)^p$ de sorte que $\mu_n(K) = \mu_m(K)$.

Ce n'est toujours pas vrai si $\mathrm{car}(K) = 0$. Par exemple, $\mu_n(\mathbb{R}) = \begin{cases} \{\pm 1\} & \text{si } n \text{ est pair} \\ \{1\} & \text{sinon.} \end{cases}$.

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

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

Définition 2.8. Le *n-ème polynôme cyclotomique* est définit par $\Phi_n = \prod_{\zeta \in \mu_n^*(\mathbb{C})} X - \zeta$.

Proposition 2.9. *Pour tout corps K, on a $X^n - 1 = \prod_{d|n} \Phi_{n,K}$.*

Démonstration. Il suffit d'observer que $\mu_n(K) = \bigsqcup_{d|n} \mu_d^*(K)$. □

Proposition 2.10. *On a $\Phi_{n,\mathbb{C}} \in \mathbb{Z}[X]$ 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 $\deg F < \deg F$ 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 $\Phi_n \in \mathbb{Z}[X]$. □

Définition 2.11. Si K est un corps et si $\iota : \mathbb{Z} \to K$ désigne le morphisme canonique, alors on définit le *n-ème polynôme cyclotomique* sur K par $\Phi_{n,K} = \iota(\Phi_n)$.

Fait 2.12. *Si $X^n - 1$ est simplement scindé sur K, alors $\Phi_{n,K} = \prod_{\zeta \in \mu_n^*(K)} X - \zeta$.*

Démonstration. On pose $\Psi_{n,k} = \prod_{\zeta \in \mu_n^*(K)} X - \zeta$. Lorsque $d|n$, le polynôme $X^d - 1$ divise $X^n - 1$ donc il est encore simplement scindé sur K. On a également $X^n - 1 = \prod_{d|n} \Psi_{d,K}$ car pour tout $d|n$, on a $\varphi(d) = \#\mu_d^*(K) = \deg \Psi_{d,K}$. On procède par récurrence sur l'ensemble des n satisfaisant l'hypothèse. Si $n = 1$, alors $\Psi_{n,K} = \Phi_{n,K} = X - 1$.

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