Mini cours Algorithmes

F-X. Dehon - 19 jan 21 - dehon@unice.fr

Algorithme :

- Suite d'instructions, éventuellement conditionnelles, éventuellement répétées un certain nombre de fois ou tant qu'une certaine condition est satisfaite, à appliquer à un certain type d'objets.

L'application pas à pas d'un algorithme à un objet donné est un calcul.

Exemple : échelonnage d'une matrice à coefficients dans un corps

> Type d'objet : $A \in \mathrm{M}_{p,q}(\mathbb{k})$
> Sortie : A échelonnée
>
> Algorithme :
> $i \leftarrow 1, j \leftarrow 1$
> tant que $i < p$ et $j \leq q$:
> $k \leftarrow i$
> tant que $k \leq p$ et $A_{k,j} = 0$: $k \leftarrow k+1$
> si $k \leq p$:
> échange $\mathrm{L}_i \leftrightarrow \mathrm{L}_k$
> pour $k \in \{i+1, \ldots, p\}$: $\mathrm{L}_k \leftarrow \mathrm{L}_k - \frac{A_{k,j}}{A_{i,j}}\mathrm{L}_i$
> $i \leftarrow i+1$
> $j \leftarrow j+1$
>
> Exemple d'application :
> ...

- Forme simplifiée : Après initiation d'un objet (valeur initiale), transformation conditionnelle de l'objet, répétée tant qu'une certaine condition est satisfaite

Exemple : division euclidienne de deux entiers

> Type d'objet : $a \in \mathbb{N},\ b \in \mathbb{N} \setminus \{0\}$
> Objet transformé : $(r,q) \in \mathbb{N}^2$ avec $a = bq + r$
>
> Algorithme :
> (r,q)$\leftarrow$(a,0)
> tant que $r > b$: (r,q)$\leftarrow$(r-b,q+1)
>
> Exemple d'application à $(a,b) = (38,17)$:
> (38,0)$\longrightarrow$(21,1)$\longrightarrow$(4,2)

Exemple : Calcul du pgcd de deux entiers par divisions euclidiennes successives

Tous nos algorithmes pourraient être mis sous cette forme au prix de complexifier le type d'objet transformé. Par exemple pour l'algorithme d'échelonnage d'une matrice, le type d'objet serait (A,i,j) avec (i,j) la position dans la matrice à partir de laquelle on commence à échelonner.

- Fonction récursive : fonction dont la définition fait appel à la fonction même mais avec un argument inférieur à l'argument de départ relativement à une certaine relation d'ordre sur les arguments.

Exemple : le reste de la division euclidienne de deux entiers

> Type d'argument : $(a,b) \in \mathbb{N} \times (\mathbb{N} \setminus \{0\})$
>
> Fonction :
> reste(a,b):=
> a si $a < b$,
> reste(a-b,b) sinon

La programmation récursive est élégante par sa concision, proche de la formulation mathématique, mais pas du tout économe en ressource de l'ordinateur (mémoire, temps de calcul) et peut parfois conduire à une programmation abérante.

Exemple : La suite de Fibonacci, cf cette page sur Wikipedia

> Type d'argument : $n \in \mathbb{N}$
>
> Fib(n):=
> 0 si n=0,
> 1 si n=1,
> Fib(n-1)+Fib(n-2) sinon

Le calcul de Fib(n) fait intervenir deux fois le calcul de Fib(n-2), cinq fois celui de Fib(n-4), etc. Mieux vaut ne faire appel qu'une seule fois à la fonction récursive dans sa définition :

> FFib(n):=
> (0,1) si n=0,
> (f2,f1+f2) où (f1,f2)=FFib(n-1) sinon
>
> Fib(n):=f1 où (f1,f2)=FFib(n)

Programmation des algorithme en Python ou Sagemath (Notice sur Wikipedia)

Sagemath = Python + nombreux types d'objets mathématiques et méthodes ou fonctions pour ces objets prédéfinis.

On peut exécuter un script Sagemath sur le site SageMathCell ou sur le site Cocalc.com (création de feuille de calcul) ou en installant le logiciel Sagemath (~1Go, ~4Go après installation !) sur son ordinateur.

Exemple :

Dans Sagemath :

```
A=matrix([[1,3],[2,4]]);print(A^(-1))
```

Le type matrice n'est pas prédéfini dans Python, il faut le définir ou importer une bibliothèque telle numpy, voir par exemple cette page de documentation.

Dans Sagemath :

```
X=GF(3)['X'].gen()
K=GF(3)['X'].quotient(X^2 + 1,'x');x=K.gen()
print(K)
print(x^2==-1)
```

définit l'anneau quotient $K = \mathbb{F}_3[X]/(X+1)$ et nomme x la classe de X dans ce quotient. Voir le test sur SageMathCell.

Pour le cours Algèbre effective, la syntaxe des commandes Sagemath utiles pour la programmation des algorithmes sera toujours donnée, sous forme d'exemples.

Instructions Sagemath

Sagemath[1] est du côté de l'utilisateur une surcouche au langage Python : le langage Python natif comme langage de programmation avec des objets structurés et des méthodes (ou fonctions) additionnels prédéfinis, tel l'objet matrice, l'opération + sur les matrices, la fonction rang, etc. : `A=matrix([[1,2],[2,4]]);print((A+A).rank())`
Un script Sagemath peut être exécuté en ligne avec SageMathCell[2] ou Cocalc[3].

Classification des instructions par niveau

0 pour les objets et méthodes premiers sans lesquels il n'y a pas de programmation : variables, listes, tests, boucles, fonctions
1 pour des objets mathématiques avec des méthodes élémentaires : entiers, matrices avec les opérations usuelles
2,3 pour une structuration et des méthodes évoluées : groupes, anneaux, espaces vectoriels, sous-objets et leurs méthodes : bases, tests d'inclusion, etc.

Ainsi dans ce qui suit :
a0, a1,... instructions pour l'arithmétique des entiers, par niveau (du plus élémentaire au plus structuré).
m1,... même chose pour les matrices.
k1,... même chose pour les groupes, anneaux, corps, anneaux de polynômes (structures algébriques)

Les niveaux servent à préciser ce qui est attendu dans un exercice. Par exemple "Ecrire un script calculant le pgcd de deux entiers avec les instructions de niveaux a1b" : on peut utiliser l'implémentation de la division euclidienne dans Sagemath mais pas la commande gcd ou équivalent (qui viderait l'exercice de son contenu).

Recherche documentaire

Voir la Quick Reference Card Sagemath pour une première liste d'objets et fonctions Sagemath. Voir bien sûr les corrigés des TP passés pour des exemples de scripts sur la page du cours L3 Algèbre effective 2016-2020.

Documentation beaucoup plus complète sur le site Sagemath et notamment cette page mais une telle documentation ne devrait pas être nécessaire pour répondre aux TP.

Et aussi la recherche sur le web par mots clefs, telle par exemple "python if condition" [4]

Programmation (Python). Voir par exemple cette page [5].

- **(0) :** mots `'123abc_'`, listes d'objets `[a,b,1,'abc']`, opération sur les listes, variable `a='1'`, fonctions `def f(a,b=1):`, boucles `for i in l:`, `while i>0:` , tests `if f(a)==[]:`, définition d'une liste par compréhension `[a for a in l if a=='1']`,
  type entier et opérations arithmétiques pour les variables d'indexation d'une liste ou d'une boucle.

Arithmétique des entiers. Voir cette Quick Reference Card. (Télécharger le pdf pour voir toutes les pages.)

- **(a1) :** type entier `0`, `13`, `ZZ`, opérations `+`, `-`, `*`, `^`v
- **a1b :** `//`, `%`, calcul modulo un entier `mod(4^8,15)`
- **(a2) :** pgcd `gcd`, fonction indicatrice d'Euler
- **(a3) :** relation de Bezout `xgcd`

Matrices. Voir la Quick Reference Card dédiée.

- **(m1) (après a1) :** liste, vecteur `vector([1,2])`, matrices `A=matrix(ZZ,[[1,2],[3,4]])`, `block_matrix()`, `identity_matrix()`, extraction `A[0,1]`, `A.row(i)`, opérations `+`, `*`, `^3`, transposée `A.transpose()` opérations sur les lignes et les colonnes `A.swap_rows(i,j)`
- **(m2) :** échelonnage, forme normale de Smith `A.echelon_form()`, `A.smith_form()`
- **(m2b) :** inverse `A^(-1)`
- **(m3) :** rang d'une matrice, déterminant, base du noyau ou de l'image, équation de l'image, solution particulière d'une équation linéaire avec second membre

Groupes, anneaux, corps, polynômes. Voir la Quick Reference Card et les tutoriels

17 mars 2021 - 28 fev 2022 - F-X. Dehon

---

1. https://www.sagemath.org/ ↩
2. https://sagecell.sagemath.org/ ↩
3. https://cocalc.com/ ↩
4. https://duckduckgo.com/?q=python+if+condition&t=h_&ia=web ↩
5. https://www.cs.put.poznan.pl/csobaniec/software/python/py-qrc.html ↩

TD 1 - Les entiers concrets, systèmes de réécritures - 22jan24

Mise à jour du 25 janvier 2024 - F-X. Dehon
Exercices prioritaires : 1.1,1.4,1.5, 2.1

❀ = Expérimentation avec Sagemath, ❀❀ marque une implémentation fastidieuse ou demandant plus d'habileté en programmation.
★ marque une question appréciée comme plus difficile ou typique d'un niveau M1, bien qu'accessible avec les connaissances de L3

On peut utiliser les mathématiques à tout niveau pour trouver une solution à un exercice ou commenter cette solution. Pour les exercices dont la réponse n'est pas immédiate on élaborera une stratégie de réponse en précisant le niveau de mathématique utilisé et on réfléchira à l'existence d'une solution élémentaire.
On répond à un exercice de programmation (marqué par ❀) en deux ou trois étapes : élaboration d'une stratégie de calcul en particulier de représentation des données, esquisse de programme ou algorithme (pseudo-code), implémentation avec Sagemath. Chaque exercice de programmation mentionne de façon plus ou moins explicite les structures de données et fonctions disponibles : si par exemple l'exercice a pour objectif le calcul du reste de la division euclidienne de a par b, les instructions `a%b` ou `a-b*(a//b)` ne sont pas des réponses satisfaisantes.

📓Notions et méthodes

- Un *entier concret* est un nombre entier explicite, tel le nombre d'éléments d'une collection explicite d'objets, par opposition au nombre abstrait : variable de type entier ou nombre donné implicitement par une propriété caractéristique.
- On désigne les entiers concrets et on calcule avec ces entiers grâce à une représentation écrite adéquate : un mot dont la valeur est explicite et ne varie pas. Cf ex.1.1 et suivants. Un calcul peut être décrit comme une suite de réécritures d'une représentation ou d'une liste de représentations d'entiers, voir plus bas et les ex. 1.1 et suivants.
- On désigne les entiers abstraits et on mène des calculs littéraux sur ces entiers en les représentant par une variable de type entier ou liste d'entiers, cf la formulation des ex.1.4 et 1.6. On fait notamment usage d'entiers abstrait pour décrire de façon formelle un calcul sur les entiers concrets, par un système de réécriture ou un script écrit dans un langage de programmation évolué tel Python. Voir un exemple ci-dessous.
- Un raisonnement sur les entiers (cf feuille 2 et suivantes), notamment une preuve de terminaison d'un algorithme de calcul sur les entiers concrets, peut également être formalisé comme une suite de réécritures d'expressions formelles suivant les règles du raisonnement, voir cet exemple de preuve avec l'assistant de preuve Edukera[1]. En général on ne fait qu'écrire une esquisse du raisonnement avec des formules traduites en langage naturel plutôt que dans le langage mathématique formel.

Système de réécritures conditionnelles

(Voir la notice Wikipedia[2] et le glossaire sur la page Moodle du cours) Il s'agit d'une liste finie de règles de réécritures d'une formule avec variables, formule qui peut être une expression algébrique ou l'expression d'une propriété, variables dont on spécialise la valeur lors d'une mise en oeuvre de la règle. L'algorithme de réécriture (ou "calcul") consiste à transformer la formule spécialisée en une donnée initiale selon les règles tant que l'une d'elles s'applique. L'algorithme se termine pour la donnée initiale si les transformations ne s'appliquent qu'un nombre fini de fois, le résultat du calcul étant alors la forme finale de la formule.
On pourra écrire une règle s'appliquant à une donnée x sous la forme
`Si <condition sur x> : x → f(x)`.
Implicitement la condition sur x et la transformation $f(x)$ sont supposées calculables en lisant une table de valeurs ou bien par un système de réécritures déjà établi.
Exemple. Avec les propriétés et opérations primitives `a=0` (test logique) `a+1` et `a-1` sur les entiers concrets, l'addition de deux entiers se calcule par le système

```
Si non b=0 : (a,b) → (a+1,b-1)
Si b=0 : (a,b) → a
```

En représentation unaire (un entier est représenté par une suite de |, l'opération +1 est l'ajout d'un |, etc.), l'exécution de ce système sur la donnée initiale (|||,||) est :
`(|||,||) → (||||,|) → (|||||,) → |||||`.
L'algorithme se termine : si b≠0 la taille de b diminue dans la transformation du couple (a,b) ; (a,0) est transformé en a qui n'est pas

un couple ; aucune règle ne s'applique à la formule a qui n'est pas un couple.
On réfléchira à la terminaison et la correction (qu'est ce que l'algorithme calcule ?), même si cet aspect sera plus systématiquement abordé dans la feuille 2.

Programmation Sagemath (= Python augmenté)[3]

Sagemath possède des objets et instructions du niveau le plus élémentaire au niveau le plus élevé, qu'on bride plus ou moins dans les exercices de programmation en spécifiant le niveau autorisé.
Objets de niveau 0 : mots `'ab'` ou `"ab"`, entiers comme symbole `0`, `1`,..., liste `['a',0,[]]`, liste d'entiers consécutifs `[1..4]`, dictionnaire `{'a':1,2:'b',c:{}}`, variables déclarées `a` (voir instruction `a=` plus loin), variables d'indice de type entier `i=1`.
Instructions de niveau 0 : affichage d'un objet `print('ab')`, déclaration-assignation d'un objet à une variable `a='ab'`, k-ième item d'une liste `l[k]`, opération sur les indices `i+1`, entrée d'un dictionnaire `l['a']` changement du k-ième item `l[k]=1`, ajout ou retrait d'un élément à une liste ou un dictionnaire `l.append('a')`, `l.remove('a')`, test d'égalité `a==b` ou de non égalité `a!=b`, opérateurs booléens `or`, `and`, `not`, instruction conditionnelle `if ...:`, boucles `while ...:`, `for`.
Objets et instructions de niveau 1 : Les entiers positifs ou négatifs, variables de type entier, opérations `+`, `-`, `*`, `//`, `%`
instructions sur les entiers de niveau 2 : `gcd(a,b)`, `xgcd(a,b)` (relation de Bezout).

L'**implémentation en Python ou Sagemath d'un système de réécritures** ressemble à :

```
x=... # donnée initiale
while cond1 or cond2 [or ...]:
    if cond1:
        x=f1(x)
    elif cond2:
        x=f2(x)
    elif...
print(x)
```

Nombre d'algorithmes de calcul évoqués dans cette feuille sont pratiqués dès l'école primaire, mais pas bien sûr l'écriture formelle de ces algorithmes (leur transcription, en particulier dans un langage de programmation, bien qu'on puisse imaginer l'utilisation d'un assistant de programmation (par exemple Scratch[4]), ni leur étude (preuve de terminaison, correction). Le discours de la méthode est intrinsèquement académique.

Systèmes de numération et premiers algorithmes

Ex.1.1 Système unaire[5] :
a. On propose ici de résumer l'expérience sensible qu'on a des entiers positifs et des calculs et relations avec les entiers par les principes suivants :

- Un entier peut être représenté par une liste de traits | ; c'est la donnée primitive.
  L'entier 0, concept pas si évident, correspond à la liste vide (qu'il faut savoir écrire autrement que par le vide lorsqu'on parle d'elle !).
- On sait structurer les données par des listes de données (les listes d'entiers devraient suffire) et bien sûr on sait lire les éléments d'une liste.
- Une fonction sur les données est représentée par la description d'une suite d'actions de lecture et d'écriture de données suivant les règles suivantes :
- On sait reconnaître qu'une liste est vide ou pas (et donc agir en conséquence).
- On sait ajouter ou retrancher un élément à une liste ; ce sont les actions primitives.
- On sait répéter une suite d'action tant qu'une condition calculable est satisfaite (boucle "while"), pourvu que cela ne dure pas trop longtemps (sinon c'est une idéalité).
- On notera si besoin Vrai, Faux les deux valeurs de vérité.

Donner des suites de réécritures permettant de calculer les relations <, = et les opérations -, ×.
❀ Implémenter en langage Sagemath ou Python votre réponse en codant un entier par une liste de 1, avec les instructions `l.append(1)`, `l.remove(1)`, avec les tests `if l == []` et `if l != []`, avec la boucle `while l!=[]` , cf l'expérimentation suivante sur SageMathCell[6] :

```
a=[1,1,1];b=[1,1]
while b != []:
    b.remove(1);
    a.append(1)
print(a)
```

Déterminer une suite de réécritures permettant de calculer la division avec reste de deux entiers.
❀ Implémenter la en langage Sagemath ou Python. L'algorithme appliqué à la liste d'entiers `[[1,1,1,1,1],[1,1]]` devrait rendre `[[1,1],[1]]`.

b. Pour réduire la longueur de la représentation des entiers, on introduit de nouveaux symboles : 5 représente un groupe de cinq 1 (une façon de coder le populaire 𝍸), 55 représente cinq 5, etc. Ainsi [55,5,5,1,1] représente l'entier 37, précédemment représenté par une liste de trente sept 1.
Spécifier un système de réécritures aboutissant à une forme "normale" ou un même mot 1 ou 5..5 ne se répète pas plus de quatre fois dans une liste représentant un entier.
Donner les valeurs dans ce système de [55,5,5,1,1]+[5,5,1,1,1,1], [55,5,5,1,1]×[5,5,1,1,1,1], [55,5,5,1,1]÷[5,1]
❀❀Comment programmeriez vous les quatre opérations +,-,×,÷ et les relations de comparaison <,= entre entiers ainsi représentés ? Penser à la réécriture, à la constitution et l'utilisation de tables de multiplication, etc.

Ex.1.2. Le système romain[7] simple est un système unaire suivi d'un regroupement par paquets suivant les règles aIIIII⟶aV, aVV⟶aX, aXXXXX⟶aL, aLL⟶aC, aCCCCC⟶aD, aDD⟶aM (où a un mot sur l'alphabet {I,V,X,L,C,D,M}) et les règles de permutation des symboles.
Soient a=XXXXII et b=XIII. Calculer a+b, a×b sans traduire le nombre dans un autre système mais en utilisant les règles de concaténation et de réécriture par paquets pour l'addition, distributivité et table de multiplication des symboles (X×V=L, etc.) pour la multiplication.
Comment calculerait on a-b ? a/b, a%b (quotient et reste de la division euclidienne) ?

Ex.1.3. On écrit un nombre entier en partant de l'écriture en batons $\mid$ (système unaire) puis en remplaçant deux batons par $\overline{\mid}$, deux symboles $\overline{\mid}$ par $\overline{\overline{\mid}}$, etc. Comment s'écrit 17 dans ce système ? Comment se compare ce système avec l'écriture binaire d'un nombre ?

Ex.1.4 (Comparer avec l'ex.1.1) On note Sa le successeur de l'entier a. Ainsi les premiers entiers sont $0, S0, SS0, SSS0, \ldots$, formules qui s'apparantent au système unaire de numération des entiers.
Pour a, b entiers on définit $a+b$ par le système de réécritures
$a+0 \to a$
$a+Sb \to Sa+b$
a. Calculer $2+3$ et $3+2$ avec la définition et la liste des écritures décimales des successeurs de 0 : [0,1,2,3,4,5,...] (par cette liste on reconnaît que 3 est le successeur de 2 ou que 2+1+1+1, le successeur itéré 3 fois de 2, s'écrit 5).
b. Avant qu'on découvre que l'opération + est associative on doit parenthéser les formules composées, telle $2+(3+2)$. Comment se calcule cette formule sans utiliser l'associativité ?
Comment peut on représenter sous forme de liste une formule parenthésée avec la seule opération + ? Comment peut on la représentée sous forme fonctionnelle sans parenthèse (Voir la notation polonaise[8]) ?

Ex.1.5. On représente un entier par la liste de ses chiffres en écriture décimale. Ainsi [3,2,4,8] désigne l'entier 3248.
a. Décrire les algorithmes établissant la comparaison < et les opérations + et × des nombres ainsi représentés, en utilisant la comparaison native des chiffres et les tables d'addition et de multiplication des chiffres, par exemple le résultat de 3×4 se lit dans la table comme [1,2] (représentant l'entier 12). Utilisez si besoin un système de retenue.
b. Décrire l'algorithme établissant l'opération - (Utilisez des retenues) et la division avec reste.
❀❀Implémenter et tester ces algorithmes en Sagemath-Python. Il pourrait être avantageux de représenter les nombres dans l'ordre inverse : [8,4,2,3] pour 3248.

Ex.1.6.a. Transcrire à la main a=8042 et b=17 (écritures décimales) en base 2 (écritures binaires).
b. Poser et faire les opérations a+b, a-b, a×b, a/b (division euclidienne) à partir des représentations binaires de a et b.
❀Proposer un algorithme pour la multiplication et la division en écriture binaire.
c. Faire la même chose avec les écritures en base 3 de a et b.
d. Comparer les longueurs des écritures d'un entier n en base 2 et en base 3.

e. Pouvez vous donner une formule pour le k-ème chiffre en partant de la droite de l'écriture en base b d'un entier positif n, en ayant à disposition la fonction reste de la division euclidienne de a par b, notée disons $a\%b$?

Calculs usuels en représentation décimale

Dans la suite on représente les entiers par leur écriture décimale et on dispose des implémentations natives des opérations usuelles +,-,×,// (quotient de la division euclidienne),% (reste de la division euclidienne) et de leurs propriétés (associativité, commutativité, distributivité, identités remarquables)

Ex.2.1. a. Calculez de tête 47×47. Quelle stratégie de calcul employez vous ?
b. Calculez à la main la division avec reste de 7237 par 38. Quelle est votre stratégie de calcul ? Comment pouvez vous tester la pertinence du résultat de votre calcul ?

Ex.2.2. Cf cette video[9]. De combien de façons peut on obtenir le nombre 74 avec les opérations +,-,× à partir des nombres 2,4,6,10 utilisés chacun au plus une fois ?
Même question avec 51 à partir des nombres 1,3,4,5,6
❀❀ Concevoir et implémenter un algorithme de recherche des solutions.

Ex.2.3. Quels chiffres des unités apparaissent dans la table de multiplication de 7 ? et de 6 ? Avec quelle régularité ? Pouvez vous en donner une explication sans former ni lire les tables en question ?

Ex.2.4. La preuve par neuf : On définit récursivement la fonction c(n) par c(n)=n si n<10 et c(n)=c(somme des chiffres de l'écriture décimale de n) sinon. La preuve par neuf conciste à vérifier après avoir calculer le produit de deux entiers a,b qu'on a c(ab)=c(c(a)c(b)).
A t-on 1832×727=1232864 ? Expliquer.
Y a t-il une preuve par neuf de la division avec reste ?
Pouvez vous concevoir une preuve par onze ? Par sept ?

Ex.2.5. a. Quelle est la longueur de la période du développement décimal de la fraction 2/13 ?
Quelles sont a priori les valeurs possibles pour la longueur de la période du développement décimal de 1/n pour n entier ≥1 ?
❀ Expérimenter avec Sagemath
b. Comment peut on définir les opérations +,-,×,/ sur les développements décimaux périodiques ?
c. Pouvez vous exhiber un développement décimal qui représentre un nombre réel non rationnel ?

Ex.2.6. ❀ (Examen mai 2022) Que rend le script Sagemath ci-dessous ? Expliquez.

```
m=[]
l=[2..100]
while l!=[]:
  m=m+[l[0]]
  l=[i for i in l if i%l[0]!=0]
print(m)
```

---

1. https://www.youtube.com/watch?v=ek3WMCJThwI ↩
2. https://en.wikipedia.org/wiki/Abstract_rewriting_system ↩
3. https://sagecell.sagemath.org/ Voir une démonstration ici : https://youtu.be/NbOKX4S51fo ↩
4. http://www.jaicompris.com/scratch/scratch_perfectionnement_suite.php ↩
5. https://fr.wikipedia.org/wiki/Système_unaire ↩
6. https://sagecell.sagemath.org/?z=eJxLtI021AHCWOskMCuWl6s8IzMnVSFJQdFWITrWipdLAQiS9IpSc_PLUjUMNa0hIol6iQUFqXkpQBFeroKizLwSjURNAAs5FCw=&lang=sage&interacts=eJyLjgUAARUAuQ== ↩
7. https://en.wikipedia.org/wiki/Roman_numerals ↩
8. https://fr.wikipedia.org/wiki/Notations_infixée,_préfixée,_polonaise_et_postfixée ↩
9. https://www.educmat.fr/categories/jeux_reflexion/fiches_jeux/le_compte_est_bon/compte1974.mp4 ↩

TD 2 - Récursion, ss-groupes de $\mathbb{Z}$, éq diophantiennes - 29jan24

Calcul littéral et raisonnement sur les entiers abstraits, ensembles d'entiers

Version du 28 janvier 2024 - F-X. Dehon
Exercices prioritaires : 1.1, 1.2a-b, 2.2, 2.3, 3.2a-e, 3.3, 4.2.

✍ = exercice de rédaction d'une preuve, le plus souvent adaptée d'une preuve vue en cours.
⚙ = structure intriquée, astucieuse (casse-tête)
❀ = Expérimentation avec Sagemath, ❀❀ marque une implémentation difficile ou fastidieuse.
★ marque une question appréciée comme plus difficile à ce niveau du cours ou typique d'un niveau M1, bien qu'accessible en L3

Notions, énoncés et méthodes

Axiomes usuels de l'arithmétique.

$\mathbb{N}$ désigne l'ensemble de tous les entiers avec un élément privilégié 0 et une fonction successeur $S : \mathbb{N} \to \mathbb{N}$ vérifiant :
- S est injective d'image $\mathbb{N} \setminus \{0\}$.
- Si P est une propriété définie sur les entiers telle qu'on a $P(0)$ et $\forall n \in \mathbb{N},\ P(n) \Rightarrow P(S(n))$ alors $P(n)$ est vrai pour tout $n \in \mathbb{N}$ (*principe de récurrence*).
On peut alors définir récursivement (voir "Récursion" ci-dessous puis l'ex.1.2) la relation de comparaison $<$, les opérations $+, \times$ etc. Une fois l'opération $+$ définie et en notant 1 le successeur de 0, $S(n)$ coïncide avec $n+1$ et on écrit habituellement $n+1$ plutôt que $S(n)$.

Récursion

- Une relation $\prec$ sur un ensemble E est dite *bien fondée* s'il n'existe pas de suite infinie d'éléments de E décroissante pour $\prec$.
Un élément $x \in E$ est dit *minimal* s'il n'existe aucun $y \in E$ tel que $y \prec x$.
- Une fonction f de E dans un ensemble F est dite *récursive* relativement à $\prec$ et une fonction $h : E \times F^{\mathcal{P}(E)} \to F$ si pour tout $x \in E$ on a $f(x) = h(x, (f(y))_{y \prec x})$.
Lorsque $x \in E$ est minimal pour $\prec$, la famille $(f(y))_{y \prec x}$ est la famille vide et la relation devient $f(x) = h(x, \emptyset)$: c'est l'initialisation de la récursion.
- Une propriété P des éléments de E est dite *héréditaire* relativement à $\prec$ si on a $\forall x \in E,\ (\forall y \prec x,\ P(y)) \Rightarrow P(x)$.
Si x est minimal pour $\prec$ l'énoncé $(\forall y \prec x,\ P(y))$ est vrai indépendamment de P donc $(\forall y \prec x,\ P(y)) \Rightarrow P(x)$ est équivalent à $P(x)$: c'est l'initialisation de l'hérédité.

Principes :
- **Preuve par récurrence :** Si $\prec$ est bien fondée alors toute propriété héréditaire sur E est vraie sur E entier.
- **Définition par récurrence :** Si $\prec$ est bien fondée alors à toute fonction h correspond une et une seule fonction récursive relativement à $\prec$ et h.
La valeur d'une formule faisant intervenir une fonction récursive f en des données explicites $x_1, \dots$ s'obtient en remplaçant autant de fois que nécessaire $f(x_i)$ par l'expression $h(x_i, (f(y))_{y \prec x_i})$ dans la formule et en évaluant ce qui peut l'être.
Exemple : le terme u_4 de la suite définie par les relations $u_0 = 0$, $u_1 = 1$ et $\forall n,\ u_{n+2} = u_n + u_{n+1}$ (cf ex.2.2) s'obtient par la suite de réécritures
$u_4 \to u_2 + u_3 \to u_0 + u_1 + u_1 + u_2 \to 2 + u_2 \to 2 + u_0 + u_1 \to 3.$

Preuve de terminaison et de correction d'un algorithme
Un algorithme est récursif s'il fait appel à lui même lors de son exécution. Un algorithme décrit par un système de réécritures est récursif (*récursif terminal*[1] précisément).
Réciproquement un algorithme récursif peut être converti en un système de réécritures (boucle while), au prix d'une complexification des variables de l'algorithme, éventuellement d'une explosion de la taille des données, cf ex.2.2 et 2.5.

On prouve la terminaison d'un algorithme récursif, en particulier de l'application d'un système de réécritures à une donnée, en cherchant une relation bien fondée sur la suite des données auquel il s'applique lors de son exécution, autrement dit en observant qu'il correspond au calcul d'une valeur prise par une fonction récursive relativement à une relation bien fondée adéquate.

❀ Implémentation d'algorithmes et expérimentations avec Sagemath.

Python permet de recopier littéralement la définition récursive des fonctions, par exemple :

```
def m(a,b):
    if a==0 or b==0:
        return(0)
    else:
        return(1+m(a-1,b-1))
```

Mais attention : une telle définition peut vite dépasser les limites de l'implémentation de Python sur machine. Essayer l'implémentation littérale de la fonction d'Ackermann définie dans l'ex.1.5 et son évaluation $A(3,9)$[2]. ($A(3,b) = 2^{b+3} - 3$ (!)) : pas de réponse dans SageMathCell, message d'erreur et remédiation proposée dans Cocalc.

Voir par exemple la page https://rosettacode.org/wiki/Ackermann_function

Le groupe $(\mathbb{Z},+)$, relation de divisibilité dans $\mathbb{Z}$:

Voir le glossaire ou les définitions dans les cours d'algèbre en L1-L2

$\mathbb{N}$ et la récurrence

Ex.1.1 ✍ **a** Montrer par récurrence ordinaire que la relation d'ordre strict habituelle $<$ sur $\mathbb{N}$ est bien fondée.
En déduire que toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
b. Inversement montrer que le principe de récurrence est conséquence du fait que toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
c. Exemple : Soit E une partie de $\mathbb{N}$ contenant 0 et stable par la fonction successeur S. Montrer $E = \mathbb{N}$.

Ex.1.2 ❀**a.** Que calcule la fonction

```
def m(a,b):
    if a==0 or b==0:return(0)
    else:return(1+m(a-1,b-1))
```

b. ✍ Donner une définition récursive de l'addition, de la soustraction et de la relation d'ordre sur les entiers ne faisant intervenir que le test d'égalité à 0, les fonctions successeur et prédécesseur, et les familles d'entiers.
Montrer que l'addition ainsi définie est commutative et associative.
Montrer l'équivalence entre $a \leq b$ et $\exists c,\ a + c = b$.
c. Donner avec les mêmes contraintes une définition récursive de la multiplication.
Montrer que la multiplication ainsi définie est commutative et associative.
❀ Tester cette définition avec Sagemath. Comment calculerait la multiplication de deux entiers avec la seule fonction successeur et des boucles "for" ?

Relation bien fondée, définitions et propriétés récursive d'une fonction

Ex.2.1 ✍Montrer par récurrence sur k que la relation d'ordre stricte $<$ associée à l'ordre lexicographique sur $\mathbb{N}^k$ est une relation bien fondée.
Qu'en est t-il de l'ordre lexicographique sur l'ensemble des familles de longueur finie d'entiers ?

Ex.2.2 La suite de Fibonacci est définie par les relations $u_0 = 0$, $u_1 = 1$ et $\forall n,\ u_{n+2} = u_n + u_{n+1}$.
a. Relativement à quelle relation bien fondée $\prec$ sur $\mathbb{N}$ et quelle fonction $h : \mathbb{N} \times \mathbb{N}^{\mathcal{P}(\mathbb{N})} \to \mathbb{N}$ la suite (u_n) vue comme fonction

$\mathbb{N} \to \mathbb{N}$ est elle récursive ?
b. Donner un système de réécriture calculant u_n à partir de la donnée initiale (n, u_0, u_1). Calculer avec ce système u_5.

Ex.2.3 ✍Montrer que la relation de divisibilité stricte sur $\mathbb{Z} \setminus \{0, -1, 1\}$: $a \prec b$ si $a \mid b$ et $b \nmid a$, est bien fondée. Quels sont les éléments minimaux ?
Montrer par récurrence relativement à cette relation que tout entier non nul s'écrit comme le produit de ± 1 et de nombres premiers.
Que se passe t-il si on considère la relation $a \prec b$ sur $\mathbb{Z} \setminus \{0\}$ entier ?

Ex.2.4 ✍Soit $(E, \prec)$, $(F, \prec)$ deux ensembles chacun muni d'une relation $\prec$. On dira que le premier est dominé par le second s'il existe une application du premier dans le second respectant $\prec$.
Montrer que si $(E, \prec)$ est dominé par $(F, \prec)$ et si la relation sur F est bien fondée alors celle sur E est également bien fondée.
Montrer que $(\mathbb{N}, <)$ est dominé par $(\mathbb{N}^2, <)$ mais pas l'inverse.
★Montrer que $(\mathbb{N}^k, <)$ est dominé par $(\mathbb{N}^l, <)$ si et seulement si $k \leq l$.

Ex.2.5 On définit la fonction d'Ackermann[3] $A : \mathbb{N}^2 \to \mathbb{N}$ par :
$A(0, n) = n + 1$
$A(m + 1, 0) = A(m, 1)$
$A(m + 1, n + 1) = A(m, A(m + 1, n))$
a. Calculer $A(2, 1)$ à la main et ❀par un script Sagemath
b. Vis a vis de quelle relation bien fondée la fonction d'Ackermann est elle récursive ?
c. Le calcul de $A(m, n)$ se termine t-il toujours ? ❀Que se passe t-il sur Sagemath ?
⚙ Déterminer un système de réécritures efficace (*i.e.* sans explosion de la taille des données) calculant $A(m, n)$.

Sous-groupes de $(\mathbb{Z}, +)$

Ex.3.1 On fixe un entier $b \neq 0$.
a. ✍ Soit $a \in \mathbb{Z}$. Observer que l'ensemble $\{a - bq,\ q \in \mathbb{Z}\} \cap \mathbb{N}$ est non vide. Montrer que le plus petit élément de cet ensemble est compris entre 0 et $|b| - 1$.
b. ✍ Montrer par récurrence sur a relativement à une relation bien fondée adéquate qu'il existe un unique $r \in \{0, \dots, b - 1\}$ tel que $a \equiv r \mod b$ (*i.e.* tel que b divise $a - r$).
Quel est le lien avec la question a ?
c. Donner un système de réécritures utilisant les tests de comparaison =,< et les opérations élémentaires +,- calculant ce plus petit élément.
Prouver la correction et la terminaison de ce calcul.

Ex.3.2 ✍
a. Soit A un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$. Montrer que l'ensemble $A \cap \mathbb{N} \setminus \{0\}$ admet un plus petit élément et que ce dernier engendre (ou génère) A. (Penser à la division euclidienne.)
b. Soient $a, b \in \mathbb{Z}$ et soit d le générateur du sous-groupe $\{ax + by,\ x, y \in \mathbb{Z}\}$ de $\mathbb{Z}$ (le sous-groupe engendré par a et b).
Montrer que d est le plus grand (pour la relation de divisibilité, cf ex.2.3) diviseur commun de a et b. On notera $d = a \wedge b$.
❀Pouvez vous écrire un algorithme de recherche naïf de ce plus grand élément ?
c. Montrer que le système de réécritures

```
(a,b) → |a|+|b| si a=0 ou b=0
(a,b) → (|a|-|b|,|b|) si 0<|b|≤|a|
(a,b) → (|a|,|b|-|a|) si 0<|a|<|b|
```

calcule $a \wedge b$, *i.e.* se termine et se termine en $a \wedge b$.
Pouvez vous adapter ce système de réécritures pour obtenir $(a \wedge b, x, y)$ avec $x, y \in \mathbb{Z}$ et $a \wedge b = ax + by$ (relation de Bézout) ?
Le couple (x, y) est il unique ?
d. On note $a//b$ et $a\%b$ le quotient et le reste de la division euclidienne de a par b (cf ex.3.1). Montrer que le système de réécritures

```
(a,b) → (b,a\%b) si $b≠0$
(a,b) → |a| si $b=0$
```

calcule $a \wedge b$. Comment adapter ce système de réécritures pour obtenir une relation de Bezout ?
e. Soient d, x, y des entiers vérifiant $ax + by = d$. Que peut on dire de d ? Que peut on dire de $x \wedge y$ (le pgcd) ?
f. Soient $a_1, \ldots, a_n \in \mathbb{Z}$ et d le générateur du sous-groupe de $\mathbb{Z}$ engendré par les a_i.
★Montrer que d peut être calculé récursivement relativement à une relation bien fondée adéquate sur $(a_1, \ldots, a_n)$. (Penser au nombre de a_i non nuls et à $\min\{|a_i|, a_i \neq 0\}$.)
Montrer que d est le plus grand (pour la relation de divisibilité) diviseur commun des a_i.
❀ Ecrire un algorithme récursif de calcul de d et d'une relation $a_1x_1 + \ldots + a_nx_n = d$.

Ex.3.3 ✍ Soient a, b deux entiers. Observer que l'intersection $a\mathbb{Z} \cap b\mathbb{Z}$ est de la forme $c\mathbb{Z}$ avec $c \geq 0$ et qu'on peut appeler c le plus petit multiple commun de a et de b. On notera $c = a \vee b$.
Pouvez vous écrire un algorithme naïf de calcul de $a \vee b$?
Montrer l'égalité $(a \wedge b)(a \vee b) = ab$.
Que peut on dire de l'intersection $a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z}$ pour $a_1, \ldots, a_n \in \mathbb{Z}$?
Quel est le générateur du sous-groupe $15\mathbb{Z} \cap 6\mathbb{Z} \cap 9\mathbb{Z} \subset \mathbb{Z}$?

Equations diophantiennes : Méthode élémentaire

Ex.4.1. ✍ Soient $a, b, c \in \mathbb{Z}$. On considère l'équation $ax + by = c$ $(*)$ d'inconnues $x, y \in \mathbb{Z}$.
a. Montrer que l'équation admet au moins une solution si et seulement si $a \wedge b$ divise c. Quelle relation y a t-il entre solution particulière de $(*)$ et relation de Bézout pour (a, b) ?
b. ★ Démontrer le lemme de Gauss : Pour $x, y, z \in \mathbb{Z}$, si x est premier avec y et divise le produit yz alors x divise z. (Utiliser une relation de Bezout.)
c. On suppose $a \wedge b = 1$. Déterminer les solutions entières de l'équation homogène $ax + by = 0$ puis un repère affine des solutions de $(*)$ à partir d'une solution particulière donnée (x_0, y_0).

Ex.4.2 a. Trouver le pgcd et une relation de Bezout pour la paire d'entiers $(12, 30)$. En déduire une solution particulière de l'équation $12x + 30y = 18$ $(*)$ d'inconnues $x, y \in \mathbb{Z}$.
b. Déterminer les solutions entières de l'équation homogène $12x + 30y = 0$ puis un repère affine des solutions de $(*)$.
c. A quelle condition sur l'entier b l'équation $12x + 30y = b$ admet elle au moins une solution ?
d. A quelle condition sur l'entier x existe t-il un entier y tel que (x, y) soit solution de $12x + 30y = 18$?
e. Trouver les $x \in \mathbb{Z}$ tels que l'équation $9x + 12y + 30z = 3$ d'inconnues y, z ait des solutions entières. Pour de tels x trouver les $y, z \in \mathbb{Z}$ solutions de $9x + 12y + 30z = 3$. En déduire un paramétrage puis un repère affine des $(x, y, z) \in \mathbb{Z}^3$ solutions de l'équation $9x + 12y + 30z = 3$.
f. Autre méthode : résoudre l'équation $(9 \wedge 12)x' + 30z = 3$ d'inconnues $x', z \in \mathbb{Z}$ puis l'équation $9x + 12y = (9 \wedge 12)x'$ d'inconnues $x, y \in \mathbb{Z}$.
Généralisation ?

Ex.4.3. On cherche une condition sur les paramètres $b, c \in \mathbb{Z}$ pour que le système d'équations ci-dessous d'inconnues $x, y, z \in \mathbb{Z}$ admette une solution entière, puis un repère affine des solutions.

$$\begin{cases} 3x + 5y = b \\ 3x + 8y + 6z = c \end{cases}$$

Méthode élémentaire : Déterminer la condition nécessaire et suffisante sur b pour que la première équation ait une solution, déterminer un paramétrage des solutions puis substituer ce paramétrage à x, y dans la seconde équation et résoudre comme en 4.2.e ou 4.2.f.

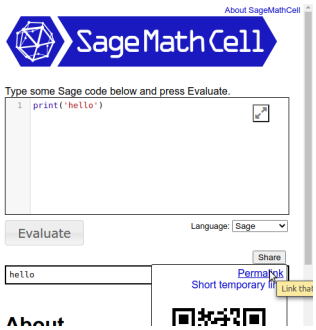
---

1. Voir récursion terminale dans la notice https://fr.wikipedia.org/wiki/Algorithme_récursif ↩
2. https://sagecell.sagemath.org/?z=eJxLSU1TSEzONTw1VHw07Ti5VJQUChKLSktylPQ8FPQVjDUVMhMU_BVsLVVMFBIzSlOVdAAqwECiDZdQx2olj8kRQg5uOG6hpqamrxcYL6xjqUmAB4aHPI=&lang=sage&interacts=eJyLjgUAARUAuQ== ↩
3. https://fr.wikipedia.org/wiki/Fonction_d'Ackermann ↩

TP 1 Listes Python, algorithmes sur les entiers - 5fev24

Répondre aux questions ci-dessous et expérimenter avec SageMathCell [1]

Lire et essayer de répondre aux questions de tête avant d'expérimenter sur machine.
Chaque script écrit dans SageMathCell peut être sauvegardé dans le corps d'un email ou dans un fichier texte bien sûr, ou bien par son permalink (cliquer sur Share, voir cette image [2]).
Pour une documentation Sagemath adaptée aux TP du cours, voir les sections "Notions et méthodes" en début des feuilles de TD et le document Instructions Sagemath [3].



Prise en main

Ex.1.1 Exécuter successivement les instructions suivantes dans SageMathCell[1:1] : `ZZ?`, `a?`, `1?`, `a=1;a?`

Ex.1.2.a Faire une recherche sur le web (avec DuckDuckGo[4] par exemple pour une recherche qui ne tienne pas compte de votre historique de navigation) sur l'expression *"sagemath définir matrice"* (sans les guillements) puis sur *"sagemath define matrix"*.
Regarder notamment les réponses (en anglais !) des forums stackexchange.com, stackoverflow.com, ask.sagemath.org[5].
Faire de même une recherche sur *"sagemath matrix construction"*, *"sagemath matrix reference"*.

b. Définir la matrice colonne de taille 10 dont les coefficients sont tous égaux à 1, puis la matrice carré $\left(\frac{1}{i+j}\right)_{1\leq i,j\leq 10}$. Vous pouvez vous aider du document "Instructions Sagemath", section "matrices" [3:1].

Listes Python

Lire la documentation Python sur les listes : construction et opérations.

Ex.2.1 On écrit les deux commandes suivantes. Que vaut v ? Comment s'interprète v comme fonction de u ?
Comparer avec l'expression mathématique $\{x,\ \exists y,\ y\in u \text{ et } x\in y\}$. Quel différence y a t-il ?

```
u=[[0,1],[4,2,1],[],[9]]
v=[x for y in u for x in y]
```

Rq. Le type ensemble existe dans Sagemath : `E=Set([4,2,1]);print(E);print(1 in E)`

Ex.2.2 Implémenter et tester les algorithmes de réécriture répondant à l'ex.1 de la feuille td 1.

Ex.2.3 On définit la fonction zo par les instructions ci-dessous. Que vaut $zo(12)$?

```
def zo(d) :
    return([x for x in [1..abs(d)] if d%x == 0])
```

Ex.2.4 Ecrire une fonction python (sans faire appel à une telle fonction déjà programmée !) prenant comme argument deux entiers a, b et rendant, si a, b ne sont pas tous deux nuls, le plus grand entier (au sens de l'ordre habituel sur $\mathbb{Z}$) qui divise à la fois a et b.
On utilisera l'instruction testant la divisibilité de a par x `a%x==0`

Programmation récursive

Ex.3.1 Que vaut $f(n)$ où f est défini ci-dessous ? Pouvez vous en donner une preuve ?

```
def f(n):
    if n%2 != 0:return(1)
    else:return(2*f(n/2))
```

Ex.3.2 La suite de Fibonacci est définie par $u_0 = 0$, $u_1 = 1$ et $\forall n,\ u_{n+2} = u_n + u_{n+1}$.
a. Définir la fonction Sagemath u (`def u(n):...` mimant litéralement la définition de la suite de Fibonnacci.
Lors de l'exécution de `u(10)` combien de fois calcule t-on $u(3)$?

Réponse[6].

b. Calculer efficacement le terme u_{97} de la suite. Cf. td2-ex2.2.

3.3 a. Cf td1-ex1.4b. Construire récursivement tous les arbres binaires planaires ayant n feuilles (pour n un entier fixé) en représentant par `[]` (la liste vide) l'arbre formé d'une seule feuille et par `[a,b]` l'arbre ayant pour bras les sous-arbres a et b. Ainsi `[[],[[],[]]]` représente l'arbre

b. On peut représenter une formule comme $a \times b$ où a et b sont eux mêmes des formules par la liste `['×',a,b]` ('×' est un code pour l'opération). Pouvez vous ainsi répondre à l'ex.2.2 de la feuille td 1 ("le compte est bon") ?

---

1. https://sagecell.sagemath.org/ ↩ ↩
2. https://math.unice.fr/~dehon/Ens/Tuto/SageMathCell.png ↩
3. https://math.unice.fr/~dehon/Ens/Sagemath/Instructions Sagemath.pdf ↩ ↩
4. https://duckduckgo.com/ ↩
5. https://duckduckgo.com/?t=h_&q=sagemath+define+matrix+site%3Aask.sagemath.org&ia=web ↩
6. https://sagecell.sagemath.org/?z=eJzzszXg5UpJTVMo1cjTtOLlUgCC9Jz8pMQcBT8ILzNNIc_W1sCqKLWktChPw0ATIpyaA5EwhEkYwiWKU6EGIbQbW_nZ-mkbIoShmoC26hpqaoMoI02gAQVFmXkIQFFDA00dP00A2FYmYw==&lang=sage&interacts=eJyLjgUAARUAuQ== ↩

TD 3 - Le groupe cyclique (ℤ/nℤ,+), sous-groupes, équations modulaires - 12fev24

Version du 13 février 2024 - F-X. Dehon
Exercices prioritaires : 1.7, 2.1, 3.*, 4.1a-b

📓 = élément de cours
✍️ = exercice de rédaction d'une preuve, le plus souvent adaptée d'une preuve vue en cours.
📌 = exercice type pour les interrogations et examens
❀ = Expérimentation avec Sagemath, ❀❀ marque une implémentation difficile ou fastidieuse.
★ marque une question appréciée comme plus difficile ou typique d'un niveau M1, bien qu'accessible en L3

📓 Notions, énoncés et méthodes

Le groupe (ℤ/nℤ,+)

- Pour n∈ℕ, ℤ/nℤ désigne l'ensemble des classes d'entiers x pour la relation de congruence notée x≡y [n] si x-y est un multiple entier de n.
  On note $\bar{x}$ la classe de l'entier x. $\bar{x}$ a un représentant privilégié : x%n le seul représentant dans l'intervalle {0,…,n-1}.
  On observe (x+y)%n≡(x%n)+(y%n) [n] et (xy)%n≡(x%n)(y%n) [n].
- L'addition des entiers induit une addition sur ℤ/nℤ : $\bar{x}+\bar{y}=\overline{x+y}$ et (ℤ/nℤ,+) est un groupe abélien fini de cardinal n.
  La multiplication des entiers induit aussi une multiplication sur ℤ/nℤ et (ℤ/nℤ,+,×) est un anneau, voir partie III du cours.
- L'application π : $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ est un homomorphisme surjectif de groupes, de noyau nℤ. C'est même un homomorphisme d'anneaux.
  L'étude des homomorphismes entre groupes ou anneaux est plutôt du niveau M1 ; on en parle quand même dans ce cours, notamment pour exprimer le théorème des restes chinois. On rappelle notamment le lemme de factorisation :
  Soit $f : A\to B$ un homomorphisme entre groupes abéliens, $K=\{x\in A, f(x)=0\}$ (le noyau de f) et L un sous-groupe de A inclus dans K. Alors f induit un homomorphisme $\bar{f} : A/L\to B$.
  $\bar{f}$ est injectif si et seulement si $L=K$. Si de plus B est fini et de même cardinal que A/L alors $\bar{f}$ est un isomorphisme.
- Le groupe ℤ/nℤ est engendré par $\bar{1}$, *i.e.* tout élément de ℤ/nℤ est multiple de $\bar{1}$; on dit que (ℤ/nℤ,+) est un groupe cyclique, d'ordre n car il est de cardinal n.
- Théorème des restes chinois : voir l'ex.4.1

Sous-groupes de (ℤ/nℤ,+)

- Il y a correspondance bijective entre les sous-groupes B ⊂ ℤ/nℤ et les sous-groupes A ⊂ ℤ contenant nℤ. La correspondance est donnée par A=π^{-1}(B), B=π(A).
  On en déduit que tout sous-groupe de ℤ/nℤ est de la forme <$\bar{d}$> avec d∈ℕ divisant n.
  Si B=<$\bar{a_1},\dots,\bar{a_q}$> alors d=pgcd($a_1,\dots,a_q$,n).
- Soit d∈ℕ divisant n, alors <$\bar{d}$> est un sous-groupe cyclique de ℤ/nℤ, d'ordre n/d.
- Pour n, a_i, x_i, b des entiers on a $a_1x_1+\cdots+a_qx_q$ ≡ b [n] si et seulement si
  ∃ k∈ℤ, $a_1x_1+\cdots+a_qx_q+nk$ = b. On se ramène ainsi à résoudre une équation linéaire avec second membre dans ℤ.
  Idem pour un système d'équations modulaires.

❀ Implémentation d'algorithmes et expérimentations avec Sagemath.

- Instruction de niveau 2 : `mod(x,n)`, cf `print(mod(-2,3).parent())`
- On utilise les matrices et leurs multiplications pour représenter un système d'équations linéaires avec second membre ou un repère affine des solutions ou une transformation linéaire des inconnues (changement de variables linéaire).
  `A=matrix([[0,1]])`, `B=matrix(1,2,{(0,1):1})`, `print(A.parent())`, `print(A*B)`, `identity_matrix(2)`, `block_matrix([[A,B],[C,D]])`, `A[:,0]`, `A[1:,:1]`, `A.nrows()`, `A.ncols()`, etc.

Révisions

Ex.1.1 Que vaut $(-2)//3$ (le quotient de la division euclidienne de -9 par 6) ?

Ex.1.2. *Cf examen et session 2 2023*
a. Calculer $12825\%35$ (le reste de la division euclidienne par 35)
b. Calculer $12825 \wedge 35$ (le plus grand diviseur commun)

Ex.1.3. Comment obtient on 180 en utilisant les nombres 4,5,6,10 au plus une fois avec les opérations +,-,× ?

Ex.1.4. ✍Soient a, b deux entiers. Montrer de façon élémentaire l'équivalence entre les deux énoncés suivants :
(1) $\exists u, v \in \mathbb{Z},\ au + bv = 1$
(2) pgcd(a,b)=1
Que peut on déduire d'une relation $au + bv = d$ quant aux relations de divisibilité entre a, b,et d ?

Ex.1.5. Donner la définition d'une relation de Bezout dans $\mathbb{Z}$. Une relation de la forme $4x + 6y = 10$ est elle une relation de Bezout ? Est elle réalisable ?

Ex.1.6 Trouver le générateur ≥ 0 du sous-groupe $< 3, 8 > \in \mathbb{Z}$ et une relation de Bézout.

Ex.1.7. Que calcule le système de réécritures ci-dessous appliqué à une famille (a_i) d'entiers ? Donnez en une preuve.
$$\begin{cases} (a_1, \ldots, a_n) \to a_1 \text{ si n=1}, \\ (a_1, \ldots, a_n) \to (a_2 \% a_1, a_1, a_3, \ldots, a_n) \text{ si n}\geq 2 \text{ et } a_1 \neq 0, \\ (a_1, \ldots, a_n) \to (a_2, a_3, \ldots, a_n) \text{ si n}\geq 2 \text{ et } a_1 = 0. \end{cases}$$

Ex.1.8.⚙ Quels algorithmes pouvez vous concevoir pour le calcul de $m \vee n$ (pour m, n entiers) ?

Ex.1.9 ❀ Ecrire une fonction Sagemath prenant en entrée la matrice et le second membre d'un système d'équations linéaires sur $\mathbb{Q}$ et rendant un repère des solutions dans $\mathbb{Q}$ du système, en raisonnant par élimination successive des inconnues du système (substitution de l'expression d'une inconnue en fonction des autres).

$\mathbb{Z}$/n$\mathbb{Z}$ et ses sous-groupes

Pour x, n deux entiers, on écrit $x\ [n]$ pour x modulo n (la classe de x dans $\mathbb{Z}/n\mathbb{Z}$ ou, pour un modèle ensembliste explicite, le sous-ensemble $x + n\mathbb{Z}$ de $\mathbb{Z}$.

Ex.2.1 ✍**a.**Montrer que tout sous-groupe B de $\mathbb{Z}/n\mathbb{Z}$ s'écrit $<\bar{d}>$ avec $d \geq 0$ divisant n. (Considérer l'image réciproque de A par $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.)
En déduire un isomorphisme entre B et $\mathbb{Z}/(n/d)\mathbb{Z}$.
b. Que vaut d pour $B =< \bar{6} > \subset \mathbb{Z}/8\mathbb{Z}$? Quel est l'ordre de 6 dans $\mathbb{Z}/8\mathbb{Z}$?
Trouver tous les $k, l \in \mathbb{Z}$ tels que $d = 6k\ [8]$ et $6 = dl\ [8]$.
c. Que vaut d pour $B =< \bar{4}, \overline{12} > \subset \mathbb{Z}/9\mathbb{Z}$?

Ex.2.2 ✍ Montrer que $\bar{x}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si x est premier avec n.

Ex.2.3 ✍ Soient n un entier et $(G, \cdot)$ un groupe pas forcément commutatif, noté multiplicativement et dont on note e le neutre. Observer que l'évaluation en $\bar{1}$ établie une correspondance bijective entre les homomorphismes $\mathbb{Z}/n\mathbb{Z} \to G$ et les éléments $g \in G$ vérifiant $g^n = e$ ($g^0 = e$ par convention).

Système d'équations modulaires

Ex.3.1 Trouver les $x \in \mathbb{Z}$ vérifiant $9x = 3\ [6]$. Quelles stratégies de calcul pouvez vous envisager ?
Idem avec les équations $9x = 3\ [15]$ d'inconnue x et $9x + 5y = 3\ [15]$ d'inconnues x, y.

Ex.3.2. a. Trouver un paramétrage affine bijectif des couples $(x, y) \in \mathbb{Z}$ solutions du système
$$\begin{cases} -3x - 2y = 1\ [9] \\ 3x - y = 2\ [6] \end{cases}$$

Méthode élémentaire : Déterminer un paramétrage des solutions de la première équation en se ramenant à une équation linéaire avec second membre sur $\mathbb{Z}$, puis reporter dans la seconde équation et poursuivre.
Le paramétrage obtenu des solutions est il bijectif ?

b. A quelle condition sur $a, b \in \mathbb{Z}$ le système d'équations ci-dessous admet il au moins une solution entière ?
Lorsque cette condition est satisfaite déterminer un paramétrage affine des $(x, y) \in \mathbb{Z}^2$ solutions.
$$\begin{cases} -3x - 2y = a\ [9] \\ 3x - y = b\ [6] \end{cases}$$

Ex.3.3. Résoudre comme en 3.2 le système :
$$\begin{cases} x \equiv 3\ [5] \\ x \equiv 4\ [13] \\ x \equiv 8\ [15] \end{cases}$$

Système de congruences, théorème des restes chinois

Ex.4.1 ✍ *Théorème des restes chinois.* Soient m, n des entiers. On considère l'homomorphisme $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $x \mapsto (x[m], x[n])$.
a. Quel est le noyau de ϕ ?
b. On suppose $m, n > 0$. Montrer que ϕ induit un isomorphisme $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
Que se passe t-il si $m = 0$ ou $n = 0$?
c. Soient $p \geq 2$ et $n_1, \dots n_p$ des entiers. Montrer que l'application $\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_p\mathbb{Z}$ est surjective si et seulement si $\mathrm{pgcd}(n_1, \dots n_p) = 1$.
Quel est son noyau ?
d. Montrer que l'application $\Psi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/(m \wedge n)\mathbb{Z}$, $(x\,[m], y\,[n]) \mapsto x - y\,[m \wedge n]$ est bien définie, $\mathbb{Z}$-linéaire (↔homomorphisme de groupe abélien) et surjective.
★e. Montrer que le noyau de Ψ s'identifie avec l'image de Φ. Que se passe t-il lorsque m et n sont premiers entre eux ?
En déduire l'égalité $(m \wedge n)(m \vee n) = mn$.
Comment prouveriez vous cette égalité de façon beaucoup plus élémentaire (en apparence en tout cas) ?

Ex.4.2. Système de congruence - méthode élémentaire.
a. ✍ Soient a, b, m, n des entiers avec $m, n > 0$. Observer que l'existence d'une solution au système d'équations
$$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$$
d'inconnue x, équivaut à celle au système échelonné d'équations diophantiennes d'inconnues x, k, l :
$$\begin{cases} x = a + km \\ km - nl = b - a \end{cases}$$
En résolvant la seconde équation et en utilisant l'exercice précédent, montrer que, pour x fixé, il existe $k, l \in \mathbb{Z}$ tels que (x, k, l) est solution de ce système ssi $m \wedge n$ divise $a - b$ et si $x \equiv c\ [m \vee n]$ pour un $c \in \mathbb{Z}$ à déterminer en fonction de a, b, m, n.

b. ✍ En déduire une manière récursive de résoudre le système de congruences d'inconnue x :
$$\begin{cases} x \equiv a_1 [n_1] \\ \vdots \\ x \equiv a_p [n_p] \end{cases}$$
❀ Implémentation Sagemath ?

Résoudre de la sorte les systèmes ci-dessous :
$$\begin{cases} x \equiv 3\ [5] \\ x \equiv 4\ [13] \\ x \equiv 8\ [15] \end{cases} \quad (1), \qquad \begin{cases} x \equiv 3\ [5] \\ x \equiv 4\ [13] \\ x \equiv 4\ [15] \end{cases}$$

Ouverture : mardi 5 mars 2024, 00:00
À remettre : dimanche 17 mars 2024, 23:00

TP2 algèbre linéaire

*Date limite pour le rendu du travail : **17 mars**.*
Document pour le TP2

Principe : vous rendez un travail abouti sur le TP2 seul ou en binôme (recommandé). Il ne s'agit pas forcément de faire la feuille en entier mais de faire un travail de qualité en un temps raisonnable.
Précisez vos sources pour votre travail (indiquer par ex. le lien vers un script trouvé sur le web ou une documentation qui vous a aidés) ; cela fait partie de la qualité de votre rendu. Indiquez ci-dessous et dans votre document les personnes qui ont participé.
Vous pouvez utiliser l'éditeur ci-dessous pour enregistrer les permalinks SageMathCell de vos scripts ou les liens vers des pages web qui vous ont aidés. Le mieux est quand-même de rendre un document pdf suivant le guide **"Mise en forme d'un travail de TP comme devoir rendu"** dans l'onglet "Calcul sur ordinateur".

Programme :
0. Lire les documents "**Instructions Sagemath**" (le même que pour le TP1) et "**Algèbre linéaire avec Sagemath**". Cf l'onglet "Calculs sur ordinateurs" sur Moodle.
1. Expérimenter (avec **SageMathCell** ou **Cocalc**) des constructeurs de matrice et instructions, notamment le code de l'ex.2.3 (forme matricielle pour relation de Bezout), ou celui des documents "**méthodes matricielle-1**" (document p3) et "**méthodes matricielle-2**" (document p4-5 ex3.7 avec forme de Smith).
2. Faire l'exercice "Exercice 3." de "Séance 5avr21" (les pages 6 et 7 du document) en utilisant la commande Sagemath `A.smith_form()`. Les stratégies sont indiquées. (La moitié du travail habituel de TP consiste à expliciter de telles stratégies.)
3. Faire l'ex. 3.9 du document : écrire sur papier la ou les stratégies, sur le modèle du point 2 ci-dessus, et implémenter - tester avec Sagemath.
4. Réfléchir aux ex. 1.2, 1.3, 2.4, 2.5, 2.12, 2.13, 2.14 de la **feuille "TD 4"**.

Ex.2.3.❀ Pour déterminer les solutions du système d'équations $\begin{cases} 3x+5y+5z=3 \\ 3x+8y+2z=0 \end{cases}$ d'inconnues $x,y,z\in\mathbb{Z}$ on a exécuté[3] le code Sagemath suivant

```
A=matrix([[3,5,5],[3,8,2]]);I=matrix([[1]])
def M(a):return(matrix(ZZ,[[0,1],[1,a]]))
Q1=block_diagonal_matrix(I,M(-1))*prod([block_diagonal_matrix(M(a),I) for a in [0,-1,-1,-2]])
Q2=prod([block_diagonal_matrix(I,M(a)) for a in [2,-2]])
show(Q1,A*Q1)
show(Q1*Q2,A*Q1*Q2)
```

```
Q1=prod([matrix(ZZ,[[0,1],[1,a]]) for a in [0,-3,-1,-2]])
Q2=matrix(ZZ,[[0,1],[1,-4]])
show("Q1=",Q1,", Q2=",Q2)
QQ1=block_diagonal_matrix(matrix([[1]]),Q1)
QQ2=block_diagonal_matrix(Q2,matrix([[1]]))
Q=QQ1*QQ2
show("QQ1=",QQ1,", QQ2=",QQ2,",Q=QQ1*QQ2=",Q)
show("(8 6 22)*Q=",matrix(1,3,[8,6,22])*Q)
```


$$Q1=\begin{pmatrix}4&-11\\-1&3\end{pmatrix},\ Q2=\begin{pmatrix}0&1\\1&-4\end{pmatrix}$$

$$QQ1=\left(\begin{array}{c|cc}1&0&0\\\hline 0&4&-11\\0&-1&3\end{array}\right),\ QQ2=\left(\begin{array}{cc|c}0&1&0\\1&-4&0\\\hline 0&0&1\end{array}\right),Q=QQ1*QQ2=\begin{pmatrix}0&1&0\\4&-16&-11\\-1&4&3\end{pmatrix}$$

$$(8\ 6\ 22)*Q=(2\quad 0\quad 0)$$

Ex.3.7. *Méthode matricielle pour les systèmes de congruences* Cf f2-ex.5.

a. 📌Montrer que le système $(1)\begin{cases}x\equiv 3\ [5]\\x\equiv 4\ [13]\\x\equiv 8\ [15]\end{cases}$ d'inconnue $x\in\mathbb{Z}$ se ramène au système $(2)\begin{cases}x+5y=3\\x+13z=4\\x+15t=8\end{cases}$ d'inconnues $x,y,z,t\in\mathbb{Z}$.

Déterminer une matrice Q inversible dans $\mathrm{M}_4(\mathbb{Z})$ telle que le produit de la matrice du système ci-dessus avec Q soit échelonnée.

En déduire les solutions du système (2) puis du système (1).

b. A quelle discussion mène cette méthode pour le système ci-dessous d'inconnue x ?

$\begin{cases}x\equiv a\ [m]\\x\equiv b\ [n]\end{cases}$

★ A quelle discussion mène cette méthode pour un système de congruences à p équations, $p\geq 1$?


```
A=matrix(ZZ,3,4,[1, 5, 0, 0, 1, 0, 13, 0, 1, 0, 0, 15])
show(A.smith_form())
D,P,Q=A.smith_form()
show("verif: PAQ=",P*A*Q)
x1,x2,x3=diagonal_matrix([1,1,1/5])*P*vector((3,4,8))
x,l=(Q*vector((x1,x2,x3,0)))[0],(Q*vector((0,0,0,1)))[0]
print("x,λ=",x,l)
print("x[λ],λ=",mod(x,l),l)
print("vérification :x[5],x[13],x[15]=",mod(x,5),mod(x,13),mod(x,15))
```


$$\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&5&0\end{pmatrix},\begin{pmatrix}0&0&1\\0&1&0\\1&0&-1\end{pmatrix},\begin{pmatrix}91&-90&0&-195\\-18&18&1&39\\-7&7&0&15\\-6&6&0&13\end{pmatrix}\right)$$

$$\texttt{verif: PAQ=}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&5&0\end{pmatrix}$$

```
x,λ= 368 -195
x[λ],λ= 173 -195
vérification :x[5],x[13],x[15]= 3 4 8
```

Séance 5avr21

lundi 5 avril 2021 13:15

Exercice 3. — Soient $u = (4, 2, 2, -3, -1)$, $v = (5, 7, -11, 3, 10)$, $w = (-1, 1, -5, 3, 4)$ des vecteurs de $\mathbf{Z}^5$. On note E le sous $\mathbf{Z}$-module de $\mathbf{Z}^5$ engendré par u, v et w.

a) Donner une base de E.

b) Le vecteur $(1, 1, -1, 0, 1)$ est-il combinaison linéaire à coefficients rationnels de u, v, w ? Est-il combinaison linéaire à coefficients entiers de u, v, w ?

c) Donner un système d'équations linéaires de E (éventuellement modulaires).

d) Soit F le sous $\mathbf{Z}$-module de $\mathbf{Z}^5$ donné par les équations

$$\begin{cases} x + 2y + z & \equiv & 0 \ [\text{mod } 5] \\ 3x + 2t & = & 0 \end{cases}$$

Donner une base de F.

e) Donner une base de $E \cap F$.

c) Stratégies :

On pause les variables, par ex (x1,x2,x3,x4,x5), qui désigneront les coordonnées d'un vecteur de $\mathbb{Z}^5$.

On résout l'équation (x1,x2,x3,x4,x5)=au+bv+cw d'inconnues a,b,c ou bien l'équation a'u'+b'v', d'inconnues a',b', où (u',v') est la base qu'on a calculé en (a).
La résolution fera apparaître une condition sur les xi sous forme d'équation linéaire, probablement modulaire, qui sera l'équation de E.

Méthodes pour cette résolution :

-> en échelonnant suivant les colonnes la matrice du système associé (cf le document "Algèbre linéaire avec Sagemath" dans le cas où l'anneau de coefficients est un corps). Sur $\mathbb{Z}$ c'est le même procédé que pour échelonné suivant les lignes : on fait apparaitre, par opérations sur les colonnes, le pgcd des coefficients d'une ligne non nulle pour l'utiliser comme pivot.

-> ou bien en passant par la forme de Smith de la matrice du système associé

d)

d) Soit F le sous $\mathbf{Z}$-module de $\mathbf{Z}^5$ donné par les équations

$$\begin{cases} x + 2y + z & \equiv & 0 \ [\text{mod } 5] \\ 3x + 2t & = & 0 \end{cases}$$

système d'équations d'inconnues x,y,z,t dans $\mathbb{Z}^5$? Il y a une inconnue cachée et un ordre implicite sur les inconnues. C'est implicitement (x,y,z,t,t') et t' n'apparait pas dans les équations, ou bien (x,y,z,s,t) et s n'apparait pas. Ce pourrait aussi être (s,t,x,y,z), etc. L'énoncé devrait le préciser.

Ce qui est sans ambiguité, c'est le calcul d'un paramétrage linéaire bijectif des (x,y,z,t) solutions.

Stratégie :
-> A la main, élémentairement par substitution des inconnues dans le reste des équations :
De la 2ème équation on a 2 divise x : x=2k puis t=-3k. On reporte dans la première équation :

2k+2y+z=0[5] ce qui équivaut à 2k+2y+z=5l pour un l∈$\mathbb{Z}$.
z=-2y-2k+5l
D'où le paramétrage des solutions :
(x,y,z,t) = (2k,y,-2y-2k+5l,-3k), y,k,l décrivant $\mathbb{Z}$.
Autrement dit l'espace vectoriel formé des (x,y,z,t) solution est isomorphe à $\mathbb{Z}^3$ via ce paramétrage. L'image de la base canonique de $\mathbb{Z}^3$ est une base ((0,-2,-2,0), (2,0,-2,-3), (0,0,5,0)) de l'espace des (x,y,z,t) solutions.

En introduisant une 5ème indéterminée fantôme t', les solutions (x,y,z,t,t') sont maintenant paramétrée de façon linéaire et bijective par y,k,l,t' :
(x,y,z,t,t') = (2k,y,-2y-2k+5l,-3k,t'), d'où la base ((0,-2,-2,0,0), (2,0,-2,-3,0), (0,0,5,0,0),(0,0,0,0,1)) de l'espace des solutions dans $\mathbb{Z}^5$. Si on considère les solutions (x,y,z,s,t) avec s fantôme, on obtient un paramétrage par y,k,l,s et la base ((0,-2,-2,0,0), (2,0,-2,0,-3), (0,0,5,0,0),(0,0,0,1,0)) de l'espace des solutions dans $\mathbb{Z}^5$.

-> en utilisant la forme de Smith
On lève la modularité de la première équation en introduisant une inconnue supplémentaire k : x+2y+z+5k=0. Un paramétrage des (x,y,z,t,k) solutions donnera, en oubliant k, un paramétrage des (x,y,z,t) solutions. Il est toujours temps ensuite d'introduire l'inconnue fantôme t' ou s, qui sera paramétrée par elle-même.

e) Base de l'intersection de E avec F.
Stratégie :

1. Faire comme en (d) mais en restreignant les (x,y,z,t,t') (ou (x,y,z,s,t) suivant le choix fait en (d)) aux vecteurs de la forme au'+bv' où (u',v') est la base de E qu'on a calculé en (a) : on obtient une base des (a,b) solutions ; l'image par l'isomorphisme de $\mathbb{Z}^2$ dans E, (a,b) ↦ au'+bv' est une base de E∩F

2. Ou bien résoudre AX=BY où A, respectivement B, est la matrice des coordonnées d'une famille génératrice de E, respectivement de F, puis calculer une base de l'image de l'application Sol → $\mathbb{Z}^5$, (X,Y) ↦ AX.

Pour des calculs à la main, (1) est plus rapide que (2) ; (2) est plus simple que (1) à implémenter avec Sagemath.

Ex.3.9. ❀Soit $A = \begin{pmatrix} -1 & 2 & 0 & -1 & -1 \\ -1 & 1 & -1 & 0 & 1 \\ 4 & 0 & -3 & 3 & 4 \\ -5 & -5 & -5 & -4 & -5 \end{pmatrix} \in \mathrm{M}_{4,5}(\mathbb{Z})$.

a. Exhiber une relation non triviale à coefficients entiers entre les colonnes de A. Qu'est ce qui garantit l'existence d'une telle relation ?

b. Exhiber un vecteur ligne $L \in \mathrm{M}_{1,5}(\mathbb{Z})$ qui ne soit pas combinaison linéaire à coefficient entier des lignes de A. Qu'est ce qui garantit l'existence de L ?

c. A t-on $\mathrm{Im}(A) = \mathbb{Z}^4$?

d. ✍Qu'est ce qui change si on se place sur $\mathbb{Q}$ plutôt que sur $\mathbb{Z}$?

On pourra utiliser cette calculatrice[3:1] avec la donnée pour A `[(-1, 2, 0, -1, -1), (-1, 1, -1, 0, 1), (4, 0, -3, 3, 4), (-5, -5, -5, -4, -5)]`
Comparer avec le rendu des instructions `A=matrix(ZZ,[(-1, 2, 0, -1, -1), (-1, 1, -1, 0, 1), (4, 0, -3, 3, 4), (-5, -5, -5, -4, -5)])`, `A.echelon_form(transformation=true)`, `A.transpose()`.

int1 - 7 mars 24

Durée : 1.25 heure. Documents et appareils électroniques interdits

Ex.1. *Calculs* — Calculer en détaillant raisonnablement :
a. -17//5 (le quotient de la division euclidienne de -17 par 5).
b. 5130%14 (le reste de la division euclidienne de 5130 par 14).
c. La liste des diviseurs entiers positifs de 14.
d. 5130∧14 (le plus grand diviseur commun de 5130 avec 14).
e. Une relation de Bezout pour le couple (5130,14).

Ex.2. *Equations* — **a.** Déterminer une solution entière particulière de l'équation
$$4x - 14y = 2$$
puis un paramétrage linéaire bijectif des solutions entières de l'équation homogène
$$4x - 14y = 0.$$
En déduire en fonction du paramètre x' un paramétrage affine des solutions entières de l'équation
$$4x - 14y = 2x'$$
d'inconnues $x, y \in \mathbb{Z}$.
A quel repère affine correspond ce paramétrage ?
Peut on trouver une solution entière à l'équation $4x - 14y = x'$ avec x' impair ?

b. Montrer que l'équation
$$4x - 14y + 9z = -1 \quad (E)$$
d'inconnues $x, y, z \in \mathbb{Z}$ se ramène au système d'équations
$$\begin{cases} 4x - 14y = 2x' \\ 2x' + 9z = -1 \end{cases}$$
d'inconnues $x', x, y, z \in \mathbb{Z}$.
En déduire avec (a) un paramétrage affine des solutions de (E).

c. Déduire de (b) un paramétrage affine des couples (x, y) d'entiers vérifiant
$$4x - 14y = -1 \bmod 9.$$

Ex.3. *Algorithme de réécritures* — On considère le système de réécritures sur les familles finies, éventuellement vides, d'entiers (éléments de $\mathbb{Z}$) :
$(a_1, \dots, a_k) \to (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_k)$ si $a_i = 0$ (on a enlevé le i-ème terme de la famille)
$(a_1, \dots, a_k) \to (a_1, \dots, a_i - a_j, \dots, a_k)$ si $i \neq j$ et $0 \neq a_j \leq a_i$ (on a remplacé le terme a_i par $a_i - a_j$)

a. Le système est il déterministe ? (*i.e.* y a t-il toujours au plus une règle qui s'applique à une famille (a_i)) ?
Quelle suite de réécritures peut on obtenir lorsqu'on applique l'algorithme de réécritures à la famille $(3, 5, 3)$? (Donner en au moins une.)

b. On définit la relation $\prec$ sur les familles d'entiers par $(a_i) \prec (b_j)$ si les a_i et b_j sont positifs ou nuls et si l'une des deux règles de réécritures transforme (b_j) en (a_i).
Montrer que la relation $\prec$ est bien fondée (*i.e.* il n'existe pas de chaîne infinie de famille d'entiers $(a_i) \succ (b_j) \succ \cdots$).
Quels sont parmi les familles d'entiers (pas forcément positifs) les éléments minimaux pour $\prec$?

c. Montrer que si $(a_i) \prec (b_j)$ alors le sous-groupe de $\mathbb{Z}$ engendré par les a_i coïncide avec le sous-groupe de $\mathbb{Z}$ engendré par les b_j, avec la convention que le sous-groupe engendré par la famille vide est $\{0\}$.

d. Que déduit on de ce qui précède quant au résultat de l'algorithme de réécritures appliqué à une famille finie d'entiers positifs ?
Que se passe t-il lorsqu'on applique l'algorithme à $(-1, 2)$?

TD 4-I - Méthodes matricielles - 11mar24

Version du 15,29 mars - F-X. Dehon

Exercices prioritaires : 1.2-5, 3.3, 3.5, 4.1a, 4.2

📓 = élément de cours ✍️ = exercice de rédaction d'une preuve, le plus souvent précisant une preuve esquissée en cours 📌 = exercice type pour les interrogations et examens ★ = question appréciée comme plus difficile à ce niveau du cours ou bien typique d'un niveau M1, bien qu'accessible en L3 ⚙ = engrenages à ajuster (casse-tête) ❀ = expérimentation avec Sagemath, ❀❀ marque une implémentation difficile ou fastidieuse.

📓Notions et méthodes

Opérations sur les lignes et les colonnes

- Soit $A \in \mathrm{M}_{p,q}(\mathbb{k})$ une matrice à coefficients dans un anneau commutatif $\mathbb{k}$. On écrit $A = \begin{pmatrix} C_1 \dots C_q \end{pmatrix}$ où C_j est la j-ième colonne de A. Une **opération élémentaire** sur les colonnes de A est de l'une des formes
  - $C_i \to C_i + aC_j$ (C_i devient $C_i + aC_j$ selon les notations de la réécriture) avec $i \neq j$ et $a \in \mathbb{k}$ quelconque,
  - $C_i \to aC_i$ avec a inversible pour la multiplication dans $\mathbb{k}$,
  - $C_i \leftrightarrow C_j$ (échange de C_i avec C_j).

  Ces opérations sont réversibles.
- Notons $\mathrm{Transf}(A, o)$ la transformation de A suivant l'opération sur les colonnes o ; on a

$$\mathrm{Transf}(A, o) = A \cdot \mathrm{Transf}(\mathrm{I}_q, o)$$

  Si $(o_1, \dots, o_k)$ est une suite d'opérations sur les colonnes qu'on applique dans l'ordre sur A alors

$$\mathrm{Transf}(A, (o_1, \dots, o_k)) = A \cdot \mathrm{Transf}(\mathrm{I}_q, (o_1, \dots, o_k)) = A \cdot \mathrm{Transf}(\mathrm{I}_q, o_1) \cdots \mathrm{Transf}(\mathrm{I}_q, o_k)$$

  Si o est réversible $Q = \mathrm{Transf}(\mathrm{I}_q, o)$ est inversible dans $\mathrm{M}_q(\mathbb{k})$ d'inverse $\mathrm{Transf}(\mathrm{I}_q, o^{-1})$.
- On définit de même les opérations élémentaires sur les lignes $L_i \to L_i + aL_j$, etc.
  Si $(o_1, \dots, o_k)$ est une suite d'opérations sur les lignes qu'on applique dans l'ordre sur A alors

$$\mathrm{Transf}(A, (o_1, \dots, o_k)) = \mathrm{Transf}(\mathrm{I}_q, (o_1, \dots, o_k)) \cdot A = \mathrm{Transf}(\mathrm{I}_q, o_k) \cdots \mathrm{Transf}(\mathrm{I}_q, o_1) \cdot A$$

  Les opérations sur les lignes sont liées aux opérations sur les colonnes via l'opération transposée $A \to {}^tA$, cf ex.1.1

Echelonnage suivant les colonnes ou les lignes

- Une matrice A est échelonnée suivant les colonnes si l'application $j \mapsto \min\{i,\ A_{i,j} \neq 0\}$ (l'indice de ligne du premier coefficient non nul de la colonne j) est strictement croissante jusqu'à être éventuellement stationnaire à $+\infty$ avec la convention $\min(\emptyset) = +\infty$.
- Pour toute matrice A il existe une suite d'opérations élémentaires sur les colonnes transformant A en une matrice échelonnée suivant les colonnes, voir l'ex.3.1 et 3.2.
- Une matrice est dite échelonnée suivant les lignes si sa transposée est échelonnée suivant les colonnes.
- **Applications :** Pour $A \in \mathrm{M}_{p,q}(\mathbb{Z})$: paramétrage des solutions entières de l'équation $AX = B$ d'inconnue X (voir ci-dessous), en particulier base de $\mathrm{Ker}(A)$ et condition sur B pour l'existence d'une solution, calcul de l'inverse à droite de A (si l'inverse existe), $\mathbb{Z}$-base de $\mathrm{Im}(A) \subset \mathbb{Z}^p$, unicité du cardinal de la base.

Equations linéaires avec second membre

- On écrit un système d'équations linéaires avec second membre sous forme matricielle $AX = B$ d'inconnue $X \in \mathrm{M}_{q,1}(\mathbb{k})$. Par opérations sur les colonnes, on ramène la résolution de $AX = B$ à celle de $(AQ)X' = B$ d'inconnue X' avec AQ échelonnée suivant les colonnes (voir les ex. 3.2 et 3.3). On observe que les solutions de $AX = B$ sont l'image par Q des solutions de $(AQ)X' = B$.
- Un paramétrage affine des solutions de $AX = B$ est la donnée d'une famille $(x_0, e_1, \dots, e_r)$ d'éléments de $\mathbb{k}^q$ tels que les solutions de $AX = B$ soient les sommes de x_0 et d'une combinaison linéaire à coefficients dans $\mathbb{k}$ des e_i (on confond ici un élément de $\mathbb{k}^q$ avec le vecteur colonne de ses coordonnées). La famille $(x_0, e_1, \dots, e_r)$ est un repère affine lorsque les e_i sont linéairement indépendants dans $\mathbb{k}^q$.

Instructions Sagemath

Constructions et instructions de **niveau 1** : vecteurs `vector([1,2])`, matrices `A=matrix(ZZ,[[1,2],[3,4]])`, `block_matrix()`, `identity_matrix()`, extraction `A[0,1]`, `A.column(i)`, opérations `+`, `*`, `A^3` (mais `A^(-1)` est de niveau 3), transposée `A.transpose()`, opérations sur les lignes et les colonnes `A.swap_columns(0,1)`, etc. Voir la Quick Reference Card dédiée[1] et le document *Algèbre linéaire avec Sagemath*[2]
Instructions de **niveau 2** : `A.echelon_form(transformation=true)` rend l'échelonnage suivant les lignes de A et la matrice de passage lorsque les coefficients de A sont de type entier (utiliser au besoin `A=matrix(ZZ,A)`). On obtient l'échelonnage suivant les colonnes via la transposée : `show([M.transpose() for M in A.transpose().echelon_form(transformation=true)])`

Opérations sur les lignes et les colonnes.

Ex.1.1 a. A quelle condition deux opérations sur les colonnes du type
$C_i \to C_i + aC_j$ avec $i \neq j$ commutent telles ?
b. Que peut on dire du déterminant d'une matrice $\mathrm{Transf}(\mathrm{I}_q, o)$ pour o une opération élémentaire sur les colonnes ?
c. Peut on réaliser l'opération $C_i \leftrightarrow C_j$ avec des opérations du type
$C_k \to C_k + aC_l$, $k \neq l$.
d. Comment s'interprète la transformation $A \to {}^tA \to \mathrm{Transf}({}^tA, o) \to {}^t\mathrm{Transf}({}^tA, o)$ pour $o = C_i \to C_i + aC_j$,
respectivement $o = C_i \to aC_i$ et $o = C_i \leftrightarrow C_j$

Ex.1.2 📓 Soit $M \in \mathrm{M}_{p,q}(\mathbb{k})$ dont on note $C_1, \dots, C_q$ les colonnes, et $u_1, \dots, u_q \in \mathbb{k}$ des scalaires. Comment s'interprète le produit $M \begin{pmatrix} u_1 \\ \vdots \\ u_q \end{pmatrix}$ en terme des C_i ?
Comment s'interprète le produit $M(\mathrm{I}_q + a\mathrm{E}_{i,j})$, où $a \in \mathbb{k}$ et $\mathrm{E}_{i,j}$ est la matrice carré de coefficient 1 en position (i,j) et 0 partout ailleurs ?
Comment s'interprète le produit $(u_1 \dots u_p)\cdot M$ en terme des lignes de M ?
Et le produit $(\mathrm{I}_p + a\mathrm{E}_{i,j})\cdot M$?

Ex.1.3. Soient $A = \begin{pmatrix} C_1 \dots C_q \end{pmatrix}$ une matrice, a, b les coefficients sur une même ligne de C_i et C_j. On suppose $b≠0. Expliciter une opération élémentaire transformant la colonne C_i de sorte que a devienne le reste $a\%b$ de la division euclidienne de a par b.

Ex.1.4 A quoi ressemble une matrice échelonnée suivant les colonnes ? Et une matrice échelonnée suivant les lignes ?

Ex.1.5. On a obtenu la matrice $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$ en transformant une matrice A suivant les opérations données ci-dessous dans l'ordre. Que vaut A ?
$C_1 \to C_1 - C_3, \quad C_2 \to C_2 - 8C_1, \quad C_3 \to C_3 - 2C_1, \quad L_1 \to L_1 + 2L_2, \quad L_1 \leftrightarrow L_2,$
$C_2 \to C_2 - 2C_3, \quad C_3 \to C_3 - 3C_2$

Relations de Bezout : approche matricielle

Ex.2.1. a. Montrer de façon élémentaire qu'une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{M}_2(\mathbb{Z})$ est inversible dans $\mathrm{M}_2(\mathbb{Z})$ si et seulement si $ad - bc = \pm 1$. Quelle est alors son inverse ?
Quel lien peut on faire avec une relation de Bézout pour le couple (a, b) ?

✍**b.** Soit $\mathbb{k}$ un anneau commutatif. Montrer qu'une matrice $A \in \mathrm{M}_n(\mathbb{k})$ est inversible dans $\mathrm{M}_n(\mathbb{k})$ si et seulement si le déterminant de A est inversible dans $\mathbb{k}$ (pour la multiplication).
Que peut on dire du pgcd des coefficients de chaque colonne de A lorsque A est inversible ?

Ex.2.2. a. Expliciter une matrice Q inversible dans $\mathrm{M}_2(\mathbb{Z})$ telle que $\begin{pmatrix} 12 & 30 \end{pmatrix} Q$ soit de la forme $\begin{pmatrix} d & 0 \end{pmatrix}$.

b. En faisant le changement de variables $\begin{pmatrix} x \\ y \end{pmatrix} = Q \begin{pmatrix} x' \\ y' \end{pmatrix}$ déterminer les solutions entières de l'équation $12x + 30y = 18$.

c. Quelles sont les matrices $Q \in \mathrm{M}_2(\mathbb{Z})$ vérifiant $\begin{pmatrix} 12 & 30 \end{pmatrix} Q = \begin{pmatrix} d & 0 \end{pmatrix}$? Quelles sont les matrices $R \in \mathrm{M}_2(\mathbb{Z})$ vérifiant $\begin{pmatrix} d & 0 \end{pmatrix} R = \begin{pmatrix} 12 & 30 \end{pmatrix}$? A t-on forcément $QR = \mathrm{I}_2$?

Echelonnage suivant les colonnes

Ex.3.1. 📓✍️ Soient $a_1, \dots, a_n, b$ des entiers.
a. Montrer (par récurrence) qu'il existe une suite d'opérations élémentaires sur les colonnes transformant la matrice ligne $\begin{pmatrix} a_1 \dots a_n \end{pmatrix}$ en $\begin{pmatrix} d\, 0 \dots 0 \end{pmatrix}$ pour un certain entier $d \geq 0$. (Cf. l'ex.3.2.f de la feuille 2.)
En déduire l'existence d'une matrice Q inversible dans $\mathrm{M}_n(\mathbb{Z})$ telle que $\begin{pmatrix} a_1 \dots a_n \end{pmatrix} Q = \begin{pmatrix} d\, 0 \dots 0 \end{pmatrix}$.
Montrer que l'entier d est le pgcd des a_i. Comment obtient on de ce qui précède une relation de Bézout $\sum_i a_i x_i = d$?

b. En déduire l'expression d'un paramétrage puis d'un repère affine des solutions entières de l'équation $a_1 x_1 + \dots + a_n x_n = b$ d'inconnues $x_1, \dots, x_n$.

Ex.3.2. 📓✍️ On définit récursivement la relation $\prec$ sur l'ensemble des matrices à coefficients dans $\mathbb{Z}$ par :

- $\begin{pmatrix} d\, 0 \dots 0 \end{pmatrix} \prec L$ pour L une matrice ligne si $d \geq 0$, $\begin{pmatrix} d\, 0 \dots 0 \end{pmatrix} \neq L$ et s'il existe une suite d'opérations élémentaires sur les colonnes transformant L en $\begin{pmatrix} d\, 0 \dots 0 \end{pmatrix}$.
- $B \prec A$ s'il existe une suite d'opérations élémentaires sur les colonnes transformant A en B (en particulier A et B ont même taille) et si de plus soit $L_1(B) \prec L_1(B)$ (où $L_1(-)$ désigne la première ligne de la matrice), soit $A = \left(\begin{array}{c|c} d & 0 \cdots 0 \\ \hline * & A_1 \end{array}\right)$, $B = \left(\begin{array}{c|c} d & 0 \cdots 0 \\ \hline * & B_1 \end{array}\right)$ avec $d \geq 0$ et $B_1 \prec A_1$.

Rq : Avec un corps commutatif, respectivement l'anneau des polynômes sur un corps, à la place de $\mathbb{Z}$ on remplacerait la condition $d \geq 0$ par $d = 1$, respectivement par d polynôme de coefficient dominant égal à 1.

a. Montrer que les éléments minimaux de $\mathrm{M}_{p,q}(\mathbb{Z})$ pour $\prec$ sont les matrices échelonnées selon les colonnes avec des coefficients de tête ≥ 0.

b.❀❀ Définir une fonction Sagemath récursive prenant comme entrée une matrice A et rendant une forme échelonnée A' de A et une matrice inversible Q telle que $A' = AQ$.

c. ⚙On peut modifier la relation $\prec$ de sorte que les éléments minimaux aient la propriété supplémentaire que les coefficients hors de la diagonale de chaque ligne i soient inférieurs strictement en valeur absolue au coefficient de la diagonale lorsque ce dernier est non nul. Quelle définition de $\prec$ convient à cet effet ?

Ex.3.3. 📓✍️ Soit $A \in \mathrm{M}_{p,q}(\mathbb{Z})$ une matrice non nulle échelonnée suivant les colonnes. On note r le nombre de colonnes non nulles.
a. Montrer que les r premières colonnes de A forment une base de $\mathrm{Im}(A)$.
b. Montrer que les $q - r$ derniers vecteurs de la base canonique de $\mathbb{Z}^q$ forment une base du noyau de A.
c. Peut on déduire de la forme de A une condition sur $B \in \mathrm{M}_{p,1}(\mathbb{Z})$ pour que l'équation $AX = B$ d'inconnue X admette au moins une solution dans $\mathrm{M}_{q,1}(\mathbb{Z})$? Comment obtient on alors une solution particulière ?
Faites les calculs avec $A = \begin{pmatrix} 5 & 0 & 0 \\ 6 & 5 & 0 \end{pmatrix}$.

Ex.3.4. ✍️ **a.** Montrer qu'une matrice $Q \in \mathrm{M}_q(\mathbb{Z})$ est inversible dans $\mathrm{M}_q(\mathbb{Z})$ si et seulement si il existe une suite d'opérations sur les colonnes transformant Q en la matrice unité I_q. Comment se calcule alors l'inverse de Q ?
b. Supposons Q de déterminant 1. Peut on transformer Q en I_q avec les seules opérations élémentaires de type $C_i \to C_i + aC_j$ avec $i \neq j$?
c. Exemple la matrice $Q = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 6 & 16 \\ 5 & 16 & 37 \end{pmatrix}$ est elle inversible ? Pouvez vous expliciter une suite d'opérations élémentaires de type $C_i \to C_i + aC_j$ avec $i \neq j$ transformant I_3 en Q ?

Ex.3.5. 📌❀ Soit $A = \begin{pmatrix} -1 & 2 & 0 & -1 & -1 \\ -1 & 1 & -1 & 0 & 1 \\ 4 & 0 & -3 & 3 & 4 \\ -5 & -5 & -5 & -4 & -5 \end{pmatrix} \in \mathrm{M}_{4,5}(\mathbb{Z})$.
a. Exhiber une relation non triviale à coefficients entiers entre les colonnes de A. Qu'est ce qui garantit l'existence d'une telle relation ?
b. Exhiber un vecteur ligne $L \in \mathrm{M}_{1,5}(\mathbb{Z})$ qui ne soit pas combinaison linéaire à coefficient entier des lignes de A. Qu'est ce qui garantit l'existence de L ?

c. A t-on $\mathrm{Im}(A) = \mathbb{Z}^4$?
d. ✍Qu'est ce qui change si on se place sur $\mathbb{Q}$ plutôt que sur $\mathbb{Z}$?

On pourra utiliser la calculatrice en ligne ech_col [3] avec la donnée pour A `[(-1, 2, 0, -1, -1), (-1, 1, -1, 0, 1), (4, 0, -3, 3, 4), (-5, -5, -5, -4, -5)]`
Comparer avec le rendu des instructions `A=matrix(ZZ,[(-1, 2, 0, -1, -1), (-1, 1, -1, 0, 1), (4, 0, -3, 3, 4), (-5, -5, -5, -4, -5)])`, `A.echelon_form(transformation=true)`, `A.transpose()`.

Méthode matricielle pour les systèmes de congruences

Ex.4.1. *Cf f3 ex3.3.* **a.** 📌 Montrer que le système $(1)\begin{cases} x \equiv 3\ [5] \\ x \equiv 4\ [13] \\ x \equiv 8\ [15] \end{cases}$ d'inconnue $x \in \mathbb{Z}$ se ramène au système

$(2)\begin{cases} x + 5y = 3 \\ x + 13z = 4 \\ x + 15t = 8 \end{cases}$ d'inconnues $x, y, z, t \in \mathbb{Z}$.

Déterminer une matrice Q inversible dans $\mathrm{M}_4(\mathbb{Z})$ telle que le produit de la matrice du système ci-dessus avec Q soit échelonnée. En déduire les solutions du système (2) puis du système (1).

b. ✍ A quelle discussion mène cette méthode pour le système ci-dessous d'inconnue x ?
$\begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases}$
★ A quelle discussion mène cette méthode pour un système de congruences à p équations, $p \geq 1$?

Ex.4.2. 📌 (Cf Interrogation d'avril 2022) Soit $A = \begin{pmatrix} 1 & 5 & 0 & 0 \\ 1 & 0 & 13 & 0 \\ 1 & 0 & 0 & 15 \end{pmatrix} \in \mathrm{M}_{3,4}(\mathbb{Z})$.
On a effectué les calculs suivants par opérations sur les colonnes :

$$A \xrightarrow[C_2 \to C_2 - 5C_1]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -5 & 13 & 0 \\ 1 & -5 & 0 & 15 \end{pmatrix} \xrightarrow[C_3 \to C_3 + 3C_2]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -5 & -2 & 0 \\ 1 & -5 & -15 & 15 \end{pmatrix} \xrightarrow[C_2 \to C_2 - 2C_3]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & -2 & 0 \\ 1 & 25 & -15 & 15 \end{pmatrix} \xrightarrow[C_3 \to C_3 - 2C_2]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 25 & -65 & 15 \end{pmatrix}$$
$$\xrightarrow[C_3 \to C_3 + 5C_4]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 25 & 10 & 15 \end{pmatrix} \xrightarrow[C_4 \to C_4 - C_3]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 25 & 10 & 5 \end{pmatrix} \xrightarrow[C_3 \to C_3 - 2C_4]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 25 & 0 & 5 \end{pmatrix} \xrightarrow[C_3 \leftrightarrow C_4]{} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 25 & 5 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[C_2 \to C_2 - 5C_1]{} \begin{pmatrix} 1 & -5 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[C_3 \to C_3 + 3C_2]{} \begin{pmatrix} 1 & -5 & -15 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[C_2 \to C_2 - 2C_3]{} \begin{pmatrix} 1 & 25 & -15 & 0 \\ 0 & -5 & 3 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \xrightarrow[C_3 \to C_3 - 2C_2]{} \begin{pmatrix} 1 & 25 & -65 & 0 \\ 0 & -5 & 13 & 0 \\ 0 & -2 & 5 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$\xrightarrow[C_3 \to C_3 + 5C_4]{} \begin{pmatrix} 1 & 25 & -65 & 0 \\ 0 & -5 & 13 & 0 \\ 0 & -2 & 5 & 0 \\ 0 & 0 & 5 & 1 \end{pmatrix} \xrightarrow[C_4 \to C_4 - C_3]{} \begin{pmatrix} 1 & 25 & -65 & 65 \\ 0 & -5 & 13 & -13 \\ 0 & -2 & 5 & -5 \\ 0 & 0 & 5 & -4 \end{pmatrix} \xrightarrow[C_3 \to C_3 - 2C_4]{} \begin{pmatrix} 1 & 25 & -195 & 65 \\ 0 & -5 & 39 & -13 \\ 0 & -2 & 15 & -5 \\ 0 & 0 & 13 & -4 \end{pmatrix} \xrightarrow[C_3 \leftrightarrow C_4]{} \begin{pmatrix} 1 & 25 & 65 & -195 \\ 0 & -5 & -13 & 39 \\ 0 & -2 & -5 & 15 \\ 0 & 0 & -4 & 13 \end{pmatrix}$$

a. Déterminer une base de $\mathrm{Im}(A)$ vu comme sous-groupe de $\mathbb{Z}^3$.
b. A quelles conditions sur $a, b, c \in \mathbb{Z}$ existe t-il $X \in \mathrm{M}_{4,1}(\mathbb{Z})$ tel que $AX = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$?
c. Déterminer un repère affine des solutions de l'équation $AX = \begin{pmatrix} 1 \\ 2 \\ 6 \end{pmatrix}$ d'inconnue X.
d. Comment s'interprète l'ensemble des entiers x tels qu'il existe des entiers y, z, t vérifiant $A \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 6 \end{pmatrix}$ en terme de relations modulaires sur x ? Déterminer cet ensemble.

---

1. (https://wiki.sagemath.org/quickref?action=AttachFile&do=view&target=quickref-linalg.pdf) ↩
2. https://math.univ-cotedazur.fr/~dehon/Ens/Sagemath/alglin-26mar20.pdf ↩
3. (https://math.unice.fr/~dehon/Ens/Nbsite/ech_col.html) ↩

TD 4-II méthode matricielle : forme de Smith - 15mar24

Version du 15 mars, 2 avril 2024 - F-X. Dehon
Exercices prioritaires : 1.2-3, 2.5, 2.7, 2.8, 2.11

📓 Notions, énoncés et méthodes

Deux notions essentielles pour cette partie :

- la variante arithmétique de l'algorithme du pivot de Gauss (qui intègre l'algorithme d'Euclide) pour obtenir la **forme normale de Smith** d'une matrice à coefficients dans un anneau euclidien ($\mathbb{Z}$ ou $\mathbb{k}[X]$) généralisant la situation des matrices à coefficients dans un corps.
- les expressions algébriques matricielles (du genre $PAQX' = PB$).

L'algorithme du pivot de Gauss et son application aux questions d'algèbre linéaire a été vu dans les deux cours de L1 Math Fondements et utilisé pour le calcul des espaces propres d'une matrice en L2-Algèbre. Les expressions algébriques matricielles apparaissent plutôt en L2.
Sur $\mathbb{Z}$ (et plus généralement sur un anneau euclidien), on peut par opérations élémentaires sur les lignes et les colonnes transformer une matrice A en une matrice nulle hors de la diagonale et dont les coefficients sur la diagonale sont positifs et croissants pour la relation de divisibilité ; c'est la **forme normale de Smith** de A. Voir l'ex.2.1.

- Pour lop est une suite d'opérations sur les lignes et les colonnes notons llop la sous-liste des opérations sur les lignes et $clop$ celle des opérations sur les colonnes alors on a

$$\mathrm{Transf}(A, lop) = \mathrm{Transf}(\mathrm{I}_p, llop) \cdot A \cdot \mathrm{Transf}(\mathrm{I}_q, clop)$$

- Une $\mathbb{Z}$-base (cf ex.1.5) d'un sous-groupe abélien de $\mathbb{Z}^n$ est dite **adaptée** si elle est une dilatation d'une $\mathbb{Z}$-base de $\mathbb{Z}^n$, cf ex.2.11b.
- Soit $A \in \mathrm{M}_{p,q}(\mathbb{Z})$; un système d'équations modulaires de $\mathrm{Im}(A)$ est un système de la forme
  $$\begin{cases} \alpha_{1,1}y_1 + \ldots + \alpha_{1,p}y_p = 0 \ [d_1] \\ \vdots \\ \alpha_{r,1}y_1 + \ldots + \alpha_{r,p}y_p = 0 \ [d_r] \end{cases}$$
  d'inconnues $y_1, \ldots, y_p$ dont $\mathrm{Im}(A)$ est l'ensemble solution. Cf ex.2.7, 2.8b

Applications de la forme normale de Smith :

Pour $A \in \mathrm{M}_{p,q}(\mathbb{Z})$: caractérisation de la classe d'équivalence de A par sa forme normale de Smith, cf ex.2.3. (deux matrices $A, B \in \mathrm{M}_{p,q}(\mathbb{Z})$ sont équivalentes s'il existe des matrices P, Q inversibles dans $\mathrm{M}_p(\mathbb{Z})$ et $\mathrm{M}_q(\mathbb{Z})$ respectivement telles que $B = PAQ$), résolution de l'équation $AX = B$ d'inconnue X cf ex.2.8, calcul d'une $\mathbb{Z}$-base de $\mathrm{Im}(A)$ *adaptée* à l'inclusion $\mathrm{Im}(A) \subset \mathbb{Z}^p$ cf ex.2.11, calcul d'un système d'équations modulaires de $\mathrm{Im}(A) \subset \mathbb{Z}^p$ cf ex.2.7 et 2.8b, complétion d'une famille de vecteurs en une base de $\mathbb{Z}^n$ (pb de la base incomplète) cf ex.2.10, description du groupe quotient $\mathbb{Z}^p/\mathrm{Im}(A)$ comme produit de groupes monogènes cf ex.2.11, classification des groupes abéliens finis.

❀ **Implémentation d'algorithmes et expérimentations avec Sagemath**.
On a besoin d'instructions adéquates pour former les matrices à partir de liste de vecteurs ligne ou colonne ou plus généralement de matrices `matrix(l)`, `column_matrix(l)`, `block_matrix(l)`. On a parfois besoin de préciser l'anneau de coefficients `matrix(ZZ,l)`.
Lorsque l'objectif n'est pas la programmation de la forme échelonnée ou de la forme de Smith, on peut utiliser l'instruction (de niveau 2) `A.smith_form()`.

Révisions

Ex.1.2 📌 *(session2-ex3c 2016-17)* Exhiber une matrice P inversible dans $\mathrm{M}_n(\mathbb{Z})$ vérifiant $\begin{pmatrix}24 & 18 & 12 & 15\end{pmatrix} P = \begin{pmatrix}d & 0 & 0 & 0\end{pmatrix}$ pour un entier d convenable.
❀ Déterminer P avec l'instruction Sagemath `A.smith_form()`.
Exhiber une $\mathbb{Z}$-base du sous-groupe $\{(x,y,z,t) \in \mathbb{Z}^4,\ dx = 0\}$ de $\mathbb{Z}^4$. En déduire une $\mathbb{Z}$-base du noyau de l'application $(x,y,z,t) \mapsto 24x + 18y + 12z + 15t$ puis un repère affine de l'ensemble des solutions de l'équation $24x + 18y + 12z + 15t = 9$.

Ex.1.3. 📌 A quelle condition sur $a, b \in \mathbb{Z}$ le système d'équations modulaires ci-dessous admet il une solution ? (Donner une équation et un paramétrage de ces couples (a, b)) Quelles sont alors les solutions ?

$$\begin{cases} x + y = a \ [6] \\ x - y = b \ [2] \end{cases}$$

❀ Réponse avec Sagemath : on peut former la matrice $\begin{pmatrix} a \\ b \end{pmatrix}$ dont les coefficients sont les paramètres symboliques a, b par les instructions `a,b=ZZ['a,b'].gens();B=matrix(2,1,[a,b])`

Ex.1.4. Chercher et appliquer une stratégie rapide de résolution à la main du système ci-dessous d'inconnues $x, y, z, t \in \mathbb{Z}$:

$$\begin{cases} 10x + 14y + 6z + 15t = 0 \\ 7x + 9y + 4z + 10t = 0 \ [2] \\ 21x + 26y + 12z + 30t = 0 \ [3] \end{cases}$$

Ex.1.5. 📓✍ *Matrice inversible et base.* Soit $\mathbb{k}$ un anneau commutatif. On dit qu'une famille $(e_1, \dots, e_q)$ d'éléments de $\mathbb{k}^n$ est une base de $\mathbb{k}^n$ si tout élément de $\mathbb{k}^n$ s'écrit de manière unique comme combinaison linéaire à coefficients dans $\mathbb{k}$ des e_i. Pour $x \in \mathbb{k}^n$ on note alors $[x]_{(e_i)}$ (ou $[x]$ si le contexte est clair) la matrice colonne des coordonnées de x dans la base (e_i).

a. Montrer que la famille (e_i) est une base si et seulement si la matrice $([e_1] \cdots [e_q]) \in \mathrm{M}_{n,q}(\mathbb{k})$ des coordonnées des e_i relativement à la base canonique est inversible à gauche et à droite.

Si $(e_1, \dots, e_q)$ et $(f_1, \dots, e_r)$ sont des bases de $\mathbb{k}^n$, comment s'écrivent les formules de changement de coordonnées en terme des matrices des coordonnées des e_i et des f_j ?

b. On suppose que $\mathbb{k}$ est un corps. Montrer que si $M \in \mathrm{M}_{n,q}(\mathbb{k})$ est inversible à gauche et à droite alors $q = n$ et l'inverse à gauche coïncide avec l'inverse à droite.

Que se passe t-il si $\mathbb{k} = \mathbb{Z}$ ou $\mathbb{Q}[X]$?

★ Que se passe t-il sans hypothèse sur $\mathbb{k}$?

Forme normale de Smith et applications

Ex.2.1. 📓✍ A une matrice $M \in \mathrm{M}_{p,q}(\mathbb{Z})$ on associe l'entier $i(M)$ égal au max des k tels que M soit diagonale par blocs

$$M = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_k & \\ \hline & 0 & & M_k \end{array}\right)$$

avec $d_i \in \mathbb{N}$, $M_k \in \mathrm{M}_{p-k,q-k}(\mathbb{Z})$ et $d_1 \mid d_2 \mid \dots \mid d_k \mid M_k$ (*i.e.* les termes sur la diagonale sont croissants pour la relation de divisibilité).

Si M est non nulle on lui associe également l'entier $m(M)$ égal au min des $|a|$, a coefficient non nul de M.

On pose $M' \prec M$ s'il existe des matrices P, Q inversibles telles que $M' = PMQ$ et si $i(M') > i(M)$ ou bien $i(M') = i(M)$ et $m(M'_{i(M')}) < m(M_{i(M)})$ (à supposé que les $m(-)$ soient bien définis).

a. Montrer l'implication $i(M) < p, q \Rightarrow \exists M', M' \prec M$ dans le cas $p = q = 2$. ★En déduit on le même résultat pour p, q quelconque ?

b. Quels sont les éléments minimaux de $\mathrm{M}_{p,q}(\mathbb{Z})$ pour la relation $\prec$? Montrer que pour toute matrice M, il existe P, Q inversibles telles que PMQ soit minimal pour $\prec$.

Ex.2.2. ✍📓 Soient M, N deux matrices à coefficients dans $\mathbb{Q}$ liées par une relation $N = PMQ$ avec P, Q matrices inversibles. Comment se compare le noyau, les bases du noyau, l'image, les bases de l'image, les équations de l'image de M et de N ? Que se passe t-il à coefficients dans $\mathbb{Z}$?

Ex.2.3. ✍📓 **a.** Soit $D \in \mathrm{M}_{p,q}(\mathbb{Z})$ une matrice nulle hors de la diagonale, de coefficients $d_1, \dots, d_r$ sur la diagonale qu'on suppose croissants pour la relation de divisibilité et soit n un entier compris entre 1 et $\min(p, q)$. Que vaut le pgcd des déterminants des matrices carrés de taille n extraites de D en fonction des d_i ?

b. Soient $n \geq 1$, $M \in \mathrm{M}_{n,n+1}(\mathbb{Z})$ et $a \in \mathbb{Z}$. Montrer que l'opération $C_1 + aC_{n+1} \to C_1$ ne change pas le pgcd des déterminants des matrices carrées de taille n extraites de M.

En déduire que le pgcd des déterminants des matrices carrées de taille n extraite d'une matrice $M \in \mathrm{M}_{p,q}(\mathbb{Z})$ ne change pas par opérations élémentaires sur les lignes ou les colonnes.

c. Déduire de ce qui précède que deux matrices sont équivalentes dans $\mathrm{M}_{p,q}(\mathbb{Z})$ si et seulement si elles ont même forme normale de Smith.

d. Montrer que la forme normale de Smith d'une matrice carré M de taille 2 est $\begin{pmatrix} d & 0 \\ 0 & \frac{|\det(M)|}{d} \end{pmatrix}$ où d est le pgcd des coefficients de M.

e. Les matrices $\begin{pmatrix} 3 & 5 & 5 \\ 3 & 8 & 2 \end{pmatrix}$ et $\begin{pmatrix} 4 & 2 & 7 \\ 2 & 4 & 4 \end{pmatrix}$ sont elles équivalentes dans $\mathrm{M}_{2,3}(\mathbb{Z})$? Et dans $\mathrm{M}_{2,3}(\mathbb{Q})$?

Ex.2.4 📌 La matrice $M = \begin{pmatrix} 8 & 3 & 3 \\ 3 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix}$ est elle inversible dans $\mathrm{M}_n(\mathbb{Z})$? Expliciter les stratégies de réponse.

Ex.2.5 📌 L'application $\mathbb{Z}^4 \to \mathbb{Z}^2,\ (x,y,z,t) \mapsto (x-y+z, x+y+3z+2t)$ est elle surjective ? A défaut pouvez vous exhiber un élément qui ne soit pas dans l'image ? Expliciter les stratégies de réponse.
❀ Utiliser Sagemath pour les calculs.

Ex.2.6 ✍️ *Forme de Smith et lemme chinois* **a.** Soient m, n deux entiers. Montrer que les conditions suivantes sont équivalentes :
(a) L'application $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\quad x\ [mn] \mapsto (x\ [m], x\ [n])$ est un isomorphisme de groupes.
(b) L'application $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\quad x \mapsto (x\ [m], x\ [n])$ est surjective
(c) L'application $\mathbb{Z}^3 \to \mathbb{Z}^2,\quad (x, q_1, q_2) \mapsto (x + q_1 m, x + q_2 n)$ est surjective
b. Montrer avec la forme de Smith que l'application du (c) est surjective si et seulement si m et n sont premiers entre eux.
c. Soient a, b deux entiers. A quelle condition sur a, b, m, n existe t-il un entier x tel que $x = a\ [m]$ et $x = b\ [n]$? Pouvez vous expliciter un tel x lorsqu'il existe ?

Ex.2.7 📌 (Examen-ex4 2019-20) On considère la matrice
$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z})$$

a. Donner une base et un système d'équations de l'image de D vue comme sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{Q}^4$ (c'est à dire lorsque D est vue comme la matrice d'une application linéaire $\mathbb{Q}^4 \to \mathbb{Q}^4$).
Donner de même une base et un système d'équations de l'image de D vue comme sous-module de $\mathbb{Z}^4$.

b. On a transformé "à la main" par opérations sur les lignes et les colonnes une matrice $A \in \mathrm{M}_4(\mathbb{Z})$ et obtenu les matrices suivantes :
$$\texttt{P} = \begin{pmatrix} -5 & -6 & -3 & -7 \\ -10 & -14 & -6 & -15 \\ 7 & 9 & 4 & 10 \\ -21 & -26 & -12 & -30 \end{pmatrix} \quad \texttt{Q} = \begin{pmatrix} -1 & 0 & -1 & 1 \\ 4 & 2 & 5 & 0 \\ -1 & -1 & -2 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \texttt{P}^{(-1)} = \begin{pmatrix} 0 & 2 & 6 & 1 \\ 0 & 0 & 3 & 1 \\ -5 & -1 & -2 & 1 \\ 2 & -1 & -6 & -2 \end{pmatrix}$$
$$\texttt{Q}^{(-1)} = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 3 & 1 & 1 & -2 \\ -2 & -1 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \texttt{P*A*Q} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$
Donner une base et un système d'équations de l'image de A d'abord vue comme sous-espace vectoriel de $\mathbb{Q}^4$ puis vue comme sous-module de $\mathbb{Z}^4$.
b-bis. Comment calculerait on une base de $\mathrm{Im}(A)$ si P^{-1} n'était pas donnée ? Cf ex.1.4.

c. *Au passage :* La matrice D est elle la forme de Smith de A ? A défaut déterminer cette forme de Smith.

Ex.2.8📌 (Examen-ex3 2020-21) Soit la matrice $A = \begin{pmatrix} 3 & 5 & 5 \\ 3 & 8 & 2 \end{pmatrix}$
a. Donner la liste des opérations sur les lignes et les colonnes transformant A en sa forme de Smith sur $\mathbb{Z}$
En déduire les matrices inversibles (dans $\mathrm{M}_n(\mathbb{Z})$) P, Q telles que PAQ soit la forme de Smith de A.
b. En déduire un système d'équations modulaires de $\mathrm{Im}(A)$ vu comme sous-groupe de $\mathbb{Z}^2$.
L'application $\mathbb{Z}^3 \to \mathbb{Z}^2$ de matrice A est elle surjective ?
Qu'en est il de l'application $\mathbb{Q}^3 \to \mathbb{Q}^2$ de matrice A ?
c. Déterminer les solutions (*i.e.* un paramétrage affine bijectif) du système d'équations d'inconnues $x, y, z \in \mathbb{Z}$:
$$\begin{cases} 3x + 5y + 5z = 3 \\ 3x + 8y + 2z = 0 \end{cases}$$
d. Soit B la matrice $B = \begin{pmatrix} 4 & 2 & 7 \\ 2 & 4 & 4 \end{pmatrix}$.

Déterminer une base du $\mathbb{Z}$-module $\mathrm{Im}(A) \cap \mathrm{Im}(B) \subset \mathbb{Z}^2$. Pouvez vous donner un élément de $\mathrm{Im}(A)$ qui ne soit pas dans $\mathrm{Im}(B)$?
❀ Utiliser Sagemath pour les calculs.

Ex.2.10 a. ✍ Soient $M \in \mathrm{M}_{n,k}(\mathbb{Z})$ avec $k < n$, (D, P, Q) la forme de Smith de M, *i.e.* D est nulle hors de la diagonale [et ses coefficients diagonaux sont en ordre croissant de divisibilité], P et Q sont inversibles et $PMQ = D$. Soit $N \in \mathrm{M}_{n,n-k}(\mathbb{Z})$; on note $(D|N)$ la matrice écrite par bloc avec N à droite de D.
Trouver P', Q' inversibles et N' telles que $P'(M|N')Q' = (D|N)$.
A quelle condition sur D et N la matrice $(D|N)$ est elle inversible ?
En déduire une condition sur D pour qu'il existe N' telle que $(M|N')$ soit inversible.
b. La famille $((1,1,2,1),(-1,1,2,1),(1,1,3,3))$ peut elle être complétée en une base de $\mathbb{Q}^4$? de $\mathbb{Z}^4$?
Compléter la famille $((1,1,2,1),(1,1,3,3))$ en une base de $\mathbb{Z}^4$.
❀ Utiliser Sagemath pour les calculs.

Ex.2.11 📌 **a.** ✍ Soient $(e_1, \ldots, e_n)$ une base de $\mathbb{Z}^n$ et $d_1 \mid \ldots \mid d_k$ des entiers en ordre croissant de divisibilité. Décrire le groupe quotient $\mathbb{Z}^n / <d_1 e_1, \ldots, d_k e_k>$ comme produit de groupes monogènes.
b. Soit A le sous-groupe de $\mathbb{Z}^2$ engendré par $(3,3)$, $(5,8)$ et $(5,2)$. Déterminer une $\mathbb{Z}$-base *adaptée* de A, c'est à dire obtenue par dilatation de certains vecteurs d'une base de $\mathbb{Z}^n$. En déduire une décomposition du groupe quotient $\mathbb{Z}^2/A$ en produit de groupes cycliques.
❀ Utiliser Sagemath pour les calculs.

Ex.2.12. ❀ Soient A et B les matrices définies par

$$A = \begin{pmatrix} 2 & 1 & 2 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & 5 & 1 \\ 0 & 0 & 3 \\ 1 & -1 & -3 \\ 2 & 4 & 3 \\ 2 & 6 & 7 \\ 4 & 6 & 2 \end{pmatrix}$$

a. Par quelles méthodes peut on décider si $\mathrm{Im}(A) = \mathrm{Im}(B)$ vus comme sous-espaces vectoriels de $\mathbb{Q}^6$? Et comme sous-$\mathbb{Z}$-modules de $\mathbb{Z}^6$?
b. Implémenter les méthodes avec Sagemath. Quelles sont les réponses ?

```
A=matrix(ZZ,[[2,-1,0,1,1,2],[1,0,-1,1,2,1],[2,1,0,2,3,3]]).transpose()
B=matrix(ZZ,[[3,0,1,2,2,4],[5,0,-1,4,6,6],[1,3,-3,3,7,2]]).transpose()
```

Ex.2.13 ❀ Soient $t \in \mathbb{Q}$ un paramètre et A la matrice de $\mathrm{M}_{6,3}(\mathbb{Q})$ définie par

$$A = \begin{pmatrix} 2 & t^2+1 & 2t^2 \\ -1 & -t & -1 \\ 0 & t^2-1 & 0 \\ 1 & 1 & -t^2+2 \\ 1 & -t+2 & -2t^2+3 \\ 2 & t+1 & -t^2+3 \end{pmatrix}$$

Discuter du rang de A suivant la valeur de t en calculant la forme de Smith de A dans $\mathbb{Q}[t]$.

```
t=QQ['t'].gen();A=matrix(QQ['t'],[[2,-1,0,1,1,2],[1+t^2,-t,t^2-1,1,2-t,1+t],[2*t^2,-1,0,2-t^2,3-2*t^2,3-t^2]]).transpose()
```

Ex.2.14 ❀ Soient A la matrice $\begin{pmatrix} 1 & 2 \\ 3 & 0 \\ 6 & 3 \end{pmatrix}$ et soient a, b, c trois paramètres. On forme $B = \left(\begin{array}{c|c} \mathbf{A} & \begin{matrix} a \\ b \\ c \end{matrix} \end{array}\right)$.
a. Essayer l'instruction `K=QQ['a,b,c'];a,b,c=K.gens();B=matrix(K,[[1,2,a],[3,0,b],[6,3,c]]);show(B.smith_form())`
Qu'en déduit on comme condition sur $a, b, c \in \mathbb{Q}$ pour que (a, b, c) soit dans $\mathrm{Im}(A)$ où A est considérée comme élément de $\mathrm{M}_{3,2}(\mathbb{Q})$?
b. ★ Pourquoi obtient on une forme de Smith de B vue dans $\mathrm{M}_{3,3}(\mathbb{Q}[a,b,c])$?
Peut on calculer une forme de Smith de B dans $\mathrm{M}_{3,3}(\mathbb{Z}[a,b,c])$?

Int2 - 4 avr 24

Durée : 1 heure. Documents et appareils électroniques interdits

Ex.1. L'application $\mathbb{Z}^4 \to \mathbb{Z}$, $(x,y,z,t) \mapsto 21x + 153y + 51z - 6t$ est elle surjective ? A défaut expliciter un entier qui n'est pas dans l'image. (Justifiez !)

Ex.2. Soit la matrice

$$A = \begin{pmatrix} 1 & -1 & 3 \\ -1 & 4 & 0 \end{pmatrix}$$

a. Donner la liste des opérations sur les lignes et les colonnes qui transforme A en sa forme de Smith sur $\mathbb{Z}$.

b. En déduire des matrices inversibles (dans $\mathrm{M}_n(\mathbb{Z})$) P, Q telles que PAQ soit la forme de Smith de A.

c. En déduire un système d'équations modulaires de $\mathrm{Im}(A)$.
L'application $\mathbb{Z}^3 \to \mathbb{Z}^2$ de matrice A est elle surjective ?

Ex.3. A quelle condition sur $(a,b) \in \mathbb{Z}^2$ le système d'équations ci-dessous d'inconnues x, y admet il au moins une solution entière (*i.e.* dans $\mathbb{Z}^2$) ? Donner cette condition sous forme d'une équation modulaire.

$$\begin{cases} x + 2y = a \bmod 4 \\ 5x + 4y = b \bmod 6 \end{cases}$$

Donner un paramétrage bijectif des couples $(x,y) \in \mathbb{Z}^2$ solutions du système pour $a = b = 1$.

Ex.4. On considère les vecteurs $e = (1,5)$ et $f = (1,2)$ de $\mathbb{Z}^2$ et on note $<2e, 6f>$ le sous-groupe de $\mathbb{Z}^2$ engendré par les vecteurs $2e$ et $6f$.
a. Le couple (e,f) est il une base de $\mathbb{Z}^2$? de $\mathbb{Q}^2$?
b. ★ Décrire le groupe quotient $A = \mathbb{Z}^2/<2e, 6f>$ comme produit de groupes cycliques.
Le groupe A est il cyclique ?
c. ★ Le groupe $B = \mathbb{Z}^2/<2e, 3f>$ est il cyclique ? Si oui pouvez vous exhiber $(x,y) \in \mathbb{Z}^2$ dont la classe modulo $<2e, 3f>$ soit générateur de B ?

TD 5 $\mathbb{Z}/n\mathbb{Z}\times$, RSA - 8avr24

Version du 10 avril 24, 15avr (ex.1.9) - F-X. Dehon
Exercices prioritaires : 1.1e, 1.2c,f, 1.4c-d, 1.9, 2.1, 2.4-6, 2.10-11, 3.3

🗒Notions, énoncés et méthodes

- On note :
  - $|E|$ le cardinal d'un ensemble E,
  - $<g_1, g_2, \dots>$ le sous-groupe d'un groupe G engendré par les éléments $g_1, g_2, \dots$ de G,
  - $\varphi(n)$ le nombre d'entiers compris entre 1 et n et premiers avec n ($n > 0$) (l'indicatrice d'Euler),
  - $m \wedge n$ et $m \vee n$ le pgcd et le ppcm de deux entiers m, n,
  - $x\ [n]$ ou $\bar{x}$ la classe d'un entier x modulo un entier n.
  - $A^\times$ le groupe multiplicatif d'un anneau A, formé des éléments inversibles pour la multiplication.
  - $\mathrm{End}(A)$ l'anneau des endomorphismes de A, c'est à dire l'ensemble des homomorphismes $A \to A$, muni de l'addition et de la composition des applications.
- On utilise :
  - Le **théorème de Lagrange** : Pour G un groupe fini et H un sous-groupe de G, $|H|$ divise $|G|$, cf ex.1.1. En particulier l'ordre d'un élément d'un groupe fini est un diviseur du cardinal du groupe.
  - Le **théorème d'Euler-Fermat** : pour toute paire d'entiers x, n premiers entre eux, $x^{\varphi(n)} \equiv 1 \bmod n$, qu'on peut voir comme un cas particulier du théorème de Lagrange.
  - Le **théorème des restes chinois** : $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est un isomorphisme lorsque m, n sont premiers entre eux, cf f2-ex.5.2, f4-ex2.6 et les ex.1.3 et 2.1 ci-dessous.
  - La **structure des sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ et les critères de cyclicité**, cf ex.1.2.
  - La **décomposition d'un groupe abélien fini** en produit de groupes cycliques d'ordres décroissants pour la relation de divisibilité, qu'on obtient algorithmiquement : voir les ex. 1.3 à 1.7.
  - La **cyclicité du groupe multiplicatif** $(\mathbb{Z}/p\mathbb{Z})^\times$ pour p un nombre premier. (Mais on ne peut pas exhiber un générateur par une formule.)
  - La **décomposition presque explicite du groupe multiplicatif** $(\mathbb{Z}/p^n\mathbb{Z})^\times$ en produit de groupes cycliques, cf ex.2.5.
- Les notions ont été en grande partie abordées en *L2-Algèbre (S4)* et *L2-Complément d'algèbre* : groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ et ses sous-groupes, produit de groupes cycliques, ordre d'un élément d'un groupe, générateurs d'un groupe cyclique, indicatrice d'Euler, anneau $\mathbb{Z}/n\mathbb{Z}$, groupe multiplicatif de l'anneau (aussi appelé groupe des unités), théorème d'Euler-Fermat, théorème des restes chinois, énoncé du théorème de décomposition d'un groupe abélien fini.
- Nombre des énoncés d'exercice ci-dessous sont des **notions de cours à connaître**, notamment ceux mentionnés plus haut ; les exercices amènent ces notions de façon on l'espère naturelle et sont l'occasion d'exercices de rédaction.
- Les **calculs** que nous avons en vue, qui sont l'objectif et la synthèse de la feuille, sont ceux des exercices 2.6c,ee (période des suites géométriques) et 3.3 (homothéties-RSA).

❀ Implémentation d'algorithmes et expérimentations avec Sagemath.

- `a=mod(2,21)` déclare `a` comme la classe de 2 dans $\mathbb{Z}/21\mathbb{Z}$. On peut alors calculer toute expression algébrique en a, notamment a^{-1} si a est inversible modulo 21, mais on ne peut pas traiter a comme un entier : `a%4` ou `gcd(a,4)` produit une erreur ; à la place `ZZ(a)` donne le représentant entier privilégié de a.
- On peut utiliser certaines instructions de niveau 2 comme `euler_phi(21)` ou `factor(21)` si l'objectif n'est pas leur programmation.
- On dispose aussi d'instructions de niveau 3-∞ (pour la curiosité, pas pour répondre aux questions), comme `a.multiplicative_order()` pour le a défini plus haut ou bien `Zmod(21).unit_group()`, `A=Zmod(7);print(A(A.unit_group().gen()))`.

Retour sur les groupes cycliques et leurs sous-groupes, et sur la décomposition des groupes abéliens finis, cf f3-ex.2.* et f4-II-ex.2.6,2.11

Ex.1.1. ✍⬚ *Théorème de Lagrange.*
Soit $(G,\cdot)$ un groupe fini de neutre noté e et soit $g\in G$. On définit récursivement g^n , $n\in\mathbb{N}$ par $g^0=e$ et $g^{n+1}=g^n\cdot g$. On pose $g^{-n}=(g^{-1})^n$, $n\in\mathbb{N}$.
a. Observer que l'application $\mathbb{Z}\to G$, $n\mapsto g^n$ est un homomorphisme de groupes d'image $<g>\subset G$ et de noyau $<d>=d\mathbb{Z}\subset\mathbb{Z}$ pour un entier $d>0$ et qu'elle induit un isomorphisme de groupes $\mathbb{Z}/d\mathbb{Z}\xrightarrow{\simeq}<g>$.
Observer $d=|<g>|$ (appelé l'ordre de g) et $g^{|<g>|}=e$.
b. Soient $(A,+)$ un groupe abélien fini et $a\in A$. Observer que la translation $\tau_a:x\mapsto a+x$ de A dans lui même est une application bijective. En déduire l'égalité $\sum_{x\in A}x=\sum_{x\in A}\tau_a(x)$ puis que $\sum_{x\in A}a=|A|a$ est nul. Reconnait on le théorème de Lagrange ?
Que peut on dire de $\sum_{x\in A}x$?
c. Soit H un sous groupe de $(G,\cdot)$. Observer que les sous-ensembles $xH=\{xh,h\in H\}$, x décrivant G, sont deux à deux égaux ou disjoints, tous de même cardinal et forment une partition de G. En déduire que le cardinal de G est multiple entier du cardinal de H.
En déduire qu'on a $\forall g\in G, g^{|G|}=e$.
d. Soient $x,n\geq 1$ deux entiers premiers entre eux. Par quelles stratégies pouvez vous démontrer le théorème d'Euler $x^{\varphi(n)}\equiv 1 \bmod n$?

Ex.1.2. ✍⬚ Soit n un entier ($n>1$). On considère le groupe additif $(\mathbb{Z}/n\mathbb{Z},+)$ qu'on dit cyclique puisqu'il est fini et admet un générateur ($\bar{1}$ est générateur). On s'intéresse à ses sous-groupes. Cf f3-ex.2.1-3.
a. Soient e un entier et f_e l'application $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, $x\mapsto e\bar{x}=\overline{ex}$.
Observer que le noyau et l'image de f_e coïncident avec ceux de $f_{e\wedge n}$ (Utiliser une relation de Bezout.), que le noyau est le sous-groupe $\frac{n}{e\wedge n}\mathbb{Z}$ de $\mathbb{Z}$ et que f_e induit un isomorphisme du groupe cyclique $\mathbb{Z}/\frac{n}{e\wedge n}\mathbb{Z}$ vers le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par e.
A quelle condition $\bar{x}$ est il générateur de $\mathbb{Z}/n\mathbb{Z}$? Observer que $\mathbb{Z}/n\mathbb{Z}$ a exactement $\varphi(n)$ générateurs.
b. Soient e un entier et h_e l'application $\mathbb{Z}/n\mathbb{Z}\circlearrowleft$, $x\mapsto ex$ (l'homothétie de rapport e). Observer que le noyau de h_e coïncide avec celui de $h_{e\wedge n}$ et que ce dernier est égal au sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de $\frac{n}{e\wedge n}$.
Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d (On a alors $d|n$). Montrer que H coïncide avec le noyau de h_d, en particulier que H est déterminé par d.
c. *Exemple :* Identifier $<\bar{8}>$ et $<\bar{8},\bar{6}>$ dans $\mathbb{Z}/12\mathbb{Z}$.
d. Montrer que pour tout diviseur d de n il y a exactement $\varphi(d)$ éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre exactement d. En déduire la formule $n=\sum_{d|n}\varphi(d)$.
❀ Implémenter la définition récursive de $\varphi(n)$ avec Sagemath.
e. Soient $d_1,\dots,d_r$ une suite d'entiers strictement positifs croissante pour la relation de divisibilité et soit $A=\mathbb{Z}/d_1\mathbb{Z}\times\cdots\times\mathbb{Z}/d_r\mathbb{Z}$.
Quel est le noyau de l'application $h_e:x\mapsto ex$ selon $e\in\mathbb{Z}$?
Montrer l'équivalence entre les conditions suivantes :
(H1) Pour tout entier k il existe au plus k éléments de A d'ordre divisant k.
(H2) $r=1$ et A est cyclique.
f.✪ Soit G un groupe fini de cardinal n ; montrer l'équivalence entre les conditions suivantes :
(H1) Pour tout diviseur d de n il existe au plus $\varphi(d)$ élément de G d'ordre exactement d.
(H2) Pour tout entier k il existe au plus k éléments de G d'ordre divisant k.
(H3) G est cyclique.
g. Exemple : les groupes $\mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ sont ils isomorphes ?

Ex.1.3. ✍ *(Cf f2-ex?.)* Soient m,n deux entiers. Construire un homomorphisme $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/(m\vee n)\mathbb{Z}$ tel que la composée $\mathbb{Z}/(m\vee n)\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/(m\vee n)\mathbb{Z}$ soit l'identité.
Indication : notons a,b les images respectives de $(1,0)$ et $(0,1)$. Etablir le système d'équations vérifiées par a,b et le résoudre. Pouvez vous déterminer la forme de Smith de la matrice du système ?
En déduire un isomorphisme $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\simeq\big(\mathbb{Z}/(m\vee n)\mathbb{Z}\big)\times\big(\mathbb{Z}/(m\wedge n)\mathbb{Z}\big)$.

Ex.1.4. a. Soit A le groupe $\mathbb{Z}/12\mathbb{Z}$. Donner la liste des éléments de A avec leurs ordres, la liste des sous-groupes de A avec pour chacun d'eux leurs générateurs. Faites un dessin 

★ Déterminer l'anneau des endomorphismes et le groupe des automorphismes de A.
b. Soit B le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Déterminer comme en (a) les ordres des éléments de B et la liste des sous-groupes de B.
Déterminer deux éléments $a, b \in B$ d'ordre 2 et 12 tels que $<a> \cap <b> = \{0\}$.
Observer que l'homomorphisme $<a> \oplus <b> \to B$, $(x, y) \mapsto x + y$ est bijectif.
★ Déteminer l'anneau des endomorphismes et le groupe des automorphismes de B. Y a t-il des automorphismes qui ne soit pas des homotheties ?
c. Avec le théorème chinois observer les isomorphismes

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \;\simeq\; \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \;\simeq\; \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\,.$$

Notons ϕ la composée de ces isomorphismes. Expliciter $\phi(1,0), \phi(0,1) \in \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ainsi que $\phi^{-1}(1,0), \phi^{-1}(0,1) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6$.
d. ⬚ Soit $(n_1, \dots, n_k)$ une famille d'entiers strictement positifs. Montrer que l'ordre d'un élément (a_i) du groupe additif $\prod_i \mathbb{Z}/n_i\mathbb{Z}$ est le ppcm des ordres de a_i dans $\mathbb{Z}/n_i\mathbb{Z}$.
Quel est l'ordre de $(2,3,4)$ dans $A = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$? Quel est l'ordre maximal d'un élément de A ? A est il cyclique ?
Quels sont les éléments d'ordre 2 dans A ? Combien y en a t-il ? Combien y en aurait il si A était cyclique ?
e. Quel est l'ordre maximal d'un élément du groupe symétrique Σ_8 (le groupe des permutations de $\{1, \dots, 8\}$) ? Penser à la décomposition d'une permutation en produit de cycles disjoints.
Y a t-il un élément d'ordre 9 dans Σ_8 ?
❀❀ En exploitant les résultats de la question (c), représenter graphiquement la suite $\left(\max\{\mathrm{o}(\sigma),\ \sigma \in \Sigma_n\}\right)_n$.

Ex.1.5. ✍⬚ Soit a, b deux éléments d'un groupe abélien $(A, +)$, d'ordres respectifs $m, n > 0$. On note $<a, b>$ le sous-groupe de A engendré par a et b ; observer que c'est l'ensemble des combinaisons linéaires $xa + yb$ à coefficients x, y entiers et que tous ses éléments sont d'ordre divisant $m \vee n$ (*i.e.* sont annulés par la multiplication par $m \vee n$).
a. On suppose pour cette question que m et n sont premiers entre eux. Montrer que $a + b$ est d'ordre mn.
b. Sans hypothèse sur m, n désormais, observer qu'on peut écrire $m = m_1 m_2$, $n = n_1 n_2$ avec $n_1 \mid m_1$, $m_2 \mid n_2$ et m_1 premier avec n_2. Observer alors $m \vee n = m_1 n_2$.
Quels sont les ordres de $m_2 a$ et de $n_1 b$? En déduire la formule d'un élément d'ordre $m \vee n$. Quel peut être l'ordre de $a + b$?

Ex.1.6 ✍ Soit $f : G \to G'$ un homomorphisme entre groupes finis et soit $g \in G$. On suppose que $f(g)$ est d'ordre k dans G' et g^k est d'ordre l dans G. Montrer que g est d'ordre kl.
Application : calcul de l'ordre de 7 dans le groupe multiplicatif $(\mathbb{Z}/5^n\mathbb{Z})^\times$, cf ex.2.6ee

Ex.1.7. ✍⬚ *Décomposition : Approche élémentaire.* Soit A un groupe abélien fini.
a. Montrer par récurrence sur la taille d'un ensemble de générateurs de A et en utilisant l'ex.1.5 qu'on peut construire un élément $a \in A$ d'ordre le ppcm des ordres des éléments de A.
b. ★ Montrer par récurrence sur la taille d'un ensemble de générateurs de A qu'on peut étendre l'application identité de $<a>$ en un homomorphisme $f : A \to <a>$.
c. ★ Montrer que l'application $A \mapsto <a> \oplus \mathrm{Ker}(f)$, $x \mapsto (f(x), x - f(x))$ est un isomorphisme (où $x - f(x)$ est défini via l'inclusion $<a> \subset A$).
En déduire par récurrence une décomposition de A en produit de groupes cycliques d'ordre décroissant pour la relation de divisibilité.
d. ★❀❀ Pouvez vous établir et implémenter un algorithme de décomposition du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ en produit de groupes cycliques suivant les idées des ex.2.1 et 2.2 ?

Ex.1.8. ✍⬚ *Décompostion via une présentation et la forme de Smith* Soit A un groupe abélien fini engendré par $a_1, \dots, a_k$ d'ordre divisant $n_1, \dots, n_k$ respectivement. (On pourrait prendre $n_1 = \dots = n_k = |A|$.)
a. Observer que l'application $f : \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \to A$, $(\bar{x}_i) \mapsto \sum_i x_i a_i$ est bien définie et est un homomorphisme surjectif.
Soit K le noyau de f et choisissons pour chaque $(\bar{x}_i) \in K$ un représentant $(x_i) \in \mathbb{Z}^k$. On note M la matrice dont les colonnes sont les vecteurs colonnes (x_i) complétée par les colonnes de la matrice diagonale de coefficients $n_1, \dots, n_k$. La matrice M a donc k lignes et $|K| + k$ colonnes.
Observer que le noyau de la composée $\mathbb{Z}^k \to \prod_i \mathbb{Z}/n_i\mathbb{Z} \xrightarrow{f} A$ coïncide avec l'image de M. En déduire via la forme de Smith de M une décomposition de A en produit de groupes cycliques d'ordre croissant pour la relation de divisibilité.
b. ❀❀ Implémenter cette méthode pour calculer une décomposition de $(\mathbb{Z}/n\mathbb{Z})^\times$ en produit de groupes cycliques, en prenant pour générateurs de $(\mathbb{Z}/n\mathbb{Z})^\times$ tous les éléments. Tester la pour $n = 15$, $n = 16$, $n = 80$. Qu'observe t-on ?
c. ★ *Alternative frugale.* On construit inductivement sur $i \in \{1, \dots, k\}$ un système de générateurs et relations de A en retenant a_i

comme générateur de A si $a_i \notin <a_1, \dots, a_{i-1}>$ et, si a_i est retenu comme générateur, en retenant une relation $da_i = \sum_{j<i, a_j \text{ est retenu}} x_j a_j$ pour $d \geq 0$ le générateur des entiers k tels que $ka_i \in <a_1, \dots, a_{i-1}>$.
Soit N la matrice dont les colonnes sont les coefficients des relations ainsi choisies entre les générateurs retenus de A. La matrice N donne t'elle une présentation de A ?
❀❀ Tester cette méthode pour calculer une décomposition de $(\mathbb{Z}/80\mathbb{Z})^\times$ en produit de groupes cycliques.

Ex.1.9. *Cf f4-II-ex.2.11 et Int2-ex.4-avr24.* Pour e, f des éléments de $\mathbb{Z}^2$ on note $<e, f>$ le sous-groupe de $\mathbb{Z}^2$ engendré par e et f.
a. Observer que (e, f) est une base de $\mathbb{Z}^2$, respectivement de $\mathbb{Q}^2$, si et seulement si la matrice $\big([e]\,[f]\big)$ des coordonnées de e et f relativement à la base canonique est inversible dans $\mathrm{M}_2(\mathbb{Z})$, respectivement dans $\mathrm{M}_2(\mathbb{Q})$.

Pour la suite on pose $e = (1, 5)$ et $f = (1, 2)$.
b. Le couple (e, f) est il une famille libre ou une base de $\mathbb{Z}^2$?
c. Montrer que l'application $(k, l) \mapsto \overline{ke + lf}$ de $\mathbb{Z}^2$ dans le groupe quotient $<e, f>/<2e, 6f>$ induit un isomorphisme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \to <e, f>/<2e, 6f>$.
d. Exhiber des entiers strictement positif m, n tels que $(m, 0)$ et $(0, n)$ soient dans $<2e, 6f>$. En déduire que le groupe quotient $A = \mathbb{Z}^2/<2e, 6f>$ est fini. Que peut on dire de son cardinal ?
e. Exhiber un couple (e', f') de vecteurs de $\mathbb{Z}^2$ et des entiers d_1, d_2 tels que $<e', f'> = \mathbb{Z}^2$ et $<d_1e', d_2f'> = <2e, 6f>$.
En déduire une décomposition de A en produit de groupes cycliques. Le groupe A est il lui même cyclique ?
f. Le groupe quotient $B = \mathbb{Z}^2/<2e, 3f>$ est il cyclique ? Si oui exhiber (x, y) dans $\mathbb{Z}^2$ dont la classe dans B soit générateur.
g. ❀ Déterminer A et B suivant l'approche des ex.1.7 et 1.8.

Le groupe multiplicatif $\mathbb{Z}/n\mathbb{Z}^\times$

Ex.2.1. $\mathbb{Z}/n\mathbb{Z}^\times$
a. Soit $n \geq 0$ et x deux entiers. Montrer l'équivalence entre :
(i) x est inversible pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$
(ii) x est premier avec n
(iii) x engendre le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$
(iv) $\exists k \geq 1,\ x^k \equiv 1\ [n]$
b. Soient $m, n \geq 1$ deux entiers tels que n soit un multiple de m. Observer que l'application $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto x\ [m]$ induit une surjection $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$.
c. *Théorème des reste chinois.* Soient $m, n \geq 1$ deux entiers premiers entre eux. Observer que l'application $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $x \mapsto (x\ [m], x\ [n])$ induit un isomorphisme d'anneaux $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et un isomorphisme de groupes $(\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.
Pouvez vous exprimer l'isomorphisme d'anneaux réciproque ?
Sans l'hypothèse m, n premiers entre eux montrer que l'application ϕ induit un isomorphisme d'anneaux $\mathbb{Z}/(m \vee n)\mathbb{Z} \to \{(a, b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ a\ [m \wedge n] = b\ [m \wedge n]\}$ (penser aux systèmes de congruences) et un isomorphisme de groupes $(\mathbb{Z}/(m \vee n)\mathbb{Z})^\times \to \{(a, b) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,\ a\ [m \wedge n] = b\ [m \wedge n]\}$.

Ex.2.2. **a.** Quels sont les générateurs de $\mathbb{Z}/15\mathbb{Z}$?
Quel est l'inverse de 86 dans $\mathbb{Z}/165\mathbb{Z}$?
b. Déterminer un paramétrage des entiers x vérifiant $86x = 4\ [165]$.

Ex.2.3. Donner la liste (sous forme paramétrée) des éléments inversibles de $\mathbb{Z}/2000\mathbb{Z}$ pour la multiplication.
❀ Tester avec Sagemath.

Ex.2.4. *Combinatoire.* Pour $n \geq 1$ entier $\varphi(n)$ désigne le nombre d'entiers compris entre 1 et n premiers avec n.
a. Observer $1 \leq \varphi(n) \leq n - 1$ si $n \geq 2$; $\varphi(n) = n - 1$ ssi n est premier.
$\varphi(p^k) = p^{k-1}(p - 1)$ si p est un nombre premier (déterminer le nombre d'éléments non premiers avec p parmi $\{0, \dots, p^k - 1\}$).
$\varphi(pq) = \varphi(p)\varphi(q)$ si p, q sont des nombres premiers distincts (déterminer l'ensemble des éléments non premiers avec p ou q parmi $\{0, \dots, pq - 1\}$).
$\varphi(pqr) = \varphi(p)\varphi(q)\varphi(r)$ si p, q, r sont des nombres premiers distincts
b. Montrer que $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont deux entiers premiers entre eux. Pouvez vous en donner une preuve purement combinatoire ?
Observer par exemple que pour x, y entiers $(nx + my)\%(mn)$ dépend bijectivement du couple $(x\%m, y\%n)$ et est premier

avec mn si et seulement si x est premier avec m et y est premier avec n.
Que se passe t-il si m et n ne sont pas premiers entre eux ?
c. Interprétation : Fixons m, n deux entiers premiers entre eux. Pour x un entier choisi au hasard les événements "x est premier avec m" et "x est premier avec n" sont indépendants. Pouvez vous donner un sens mathématiques précis à ce slogan ?
Si m et n ne sont pas premiers entre eux, l'événement "x est premier avec m" rend il plus ou moins probable l'événement "x est premier avec n" ?
c. Comment se calcule $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n ?
★ Qu'en déduit on sur le sup et l'inf dans $\mathbb{R}$ de l'ensemble $\{\frac{\varphi(k)}{k},\ k > n\}$ (en fonction de n) ?
d. Pouvez vous donner quatre entiers n tels que $\varphi(n) = 48$?
e. ❀ Répondre naïvement avec Sagemath : Quelle est la liste de éléments inversibles de $\mathbb{Z}/165\mathbb{Z}$? L'application $n \mapsto \varphi(n)$ semble t-elle injective ? croissante ? La suite $\left(\log(\frac{\varphi(n)}{n})\right)_n$ semble t-elle bornée ?

Ex.2.5. ✍ **a.** Soient A un anneau commutatif intègre, P un polynôme à coefficients dans A et $a_1, \dots, a_n$ n racines distinctes de P. Montrer que $(X - a_1) \cdots (X - a_n)$ divise P et donc $n \leq \deg(P)$.
[Contre-] exemple : 1. Prenons pour A l'anneau produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $P = X^2 - 1$. Quelles sont les racines de P dans A ? Quelle factorisations de P peut on avoir dans $A[X]$?
2. Mêmes questions pour $A = \mathbb{Z}/8\mathbb{Z}$.
b. On suppose toujours A intègre. Soit G un sous groupe fini du groupe multiplicatif $A^\times$. Montrer que G est cyclique. (Utiliser l'exercice 1.2.)
Exemple : Pour p entier premier le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.
Qu'en est il de $(\mathbb{Z}/pq\mathbb{Z})^\times$ pour p, q deux entiers premiers distincts ?
Qu'en est il de $(\mathbb{Z}/9\mathbb{Z})^\times$?
c. Quels sont les entiers n tels que $\mathbb{Z}/n\mathbb{Z}$ est intègre ?
d.★ Que peut on dire du lien entre degré et nombre de racines pour $A = \mathbb{Z}/p^k\mathbb{Z}$, p premier ?

Ex.2.6. ✍ Soit $p > 2$ un nombre premier et $n > 0$ un entier. On considère le groupe multiplicatif $(\mathbb{Z}/p^n\mathbb{Z})^\times$
a. Quels sont les ordres plausibles des éléments de $(\mathbb{Z}/p^n\mathbb{Z})^\times$?
Observer que la réduction modulo p induit un homomorphisme surjectif $(\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ (cf ex.2.1). En déduire l'existence d'un élément y de $(\mathbb{Z}/p^n\mathbb{Z})^\times$ d'ordre $p - 1$.
b. Soit K le noyau de l'application $(\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Quel est son cardinal ? Observer que K est formé des éléments de la forme $1 + \lambda p\ [p^n]$ avec λ entier.
Montrer que pour $k \geq 1$ et pour λ un entier premier avec p on a $(1 + \lambda p^k)^p = 1 + \mu p^{k+1}$ avec μ premier à p. (Utilisez la formule du binôme.) Que se passe t-il si $p = 2$?
En déduire que $1 + \lambda p^k\ [p^n]$ est d'ordre p^{n-k} dans $(\mathbb{Z}/p^n\mathbb{Z})^\times$ puis que K est engendré par $1 + p$.
⚙Pouvez vous expliciter, pour $k \geq 1$ et pour λ un entier premier avec p, un entier $l \geq 1$ tel que $(1 + p)^l = 1 + \lambda p^k\ [p^n]$?
c. Déduire de ce qui précède que le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique.
Pouvez vous exhiber un générateur de $(\mathbb{Z}/3^{10}\mathbb{Z})^\times$?
⚙ Quel est l'ordre de 7 dans $(\mathbb{Z}/5^n\mathbb{Z})^\times$ en fonction de n ? (Utiliser l'ex.1.6.) ❀ Vérifiez avec Sagemath.
d. Cas $p = 2$: Montrer que l'homomorphisme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z} \to \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times$, $(1, 0) \mapsto -1$, $(0, 1) \mapsto 5$ est bijectif.
e. Pour quels entiers n a t-on $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ cyclique ?
f. Les groupes $(\mathbb{Z}/n\mathbb{Z})^\times$ pour les entiers n de la question 2.4d sont ils isomorphes ?
ee.⚙ On considère la suite $(\bar{7}^n)_n$ dans l'anneau $\mathbb{Z}/(105^5)\mathbb{Z}$. A partir de quel rang devient elle périodique ? Quel est alors sa période ?
❀ Vérifiez votre réponse avec Sagemath (cf le sujet du TP3).

Ex.2.7.★ Soit x un entier fixé. L'affirmation "la probabilité que x soit générateur du groupe "$(\mathbb{Z}/p\mathbb{Z})^\times$ pour p un nombre premier pris au hasard est $\frac{\varphi(p-1)}{p-1}$" vous parait elle raisonnable ?
Que se passe t-il si $x = 4$? Si $x = 2$?

Ex.2.8 Soit x la classe de 5 dans $\mathbb{Z}/(30^{10})\mathbb{Z}$
A partir de quel rang la suite $(x^n)_n$ est elle périodique ? Quelle est alors sa période ?

Ex.2.9 📌 Déterminer une décomposition de $(\mathbb{Z}/165\mathbb{Z})^\times$ en produit de groupes cycliques.

Ex.2.10 📌 *(Int1 mars 2021)* **a.** Quels sont les ordres possibles d'un élément du groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^\times$? Quel est l'ordre de 2 dans ce groupe ?

b. Quel est l'ordre de 86 dans $(\mathbb{Z}/165\mathbb{Z})^\times$?
❀ Déterminer naïvement avec Sagemath les ordres pour la multiplication des éléments inversibles de $\mathbb{Z}/165\mathbb{Z}$. Le groupe $(\mathbb{Z}/165\mathbb{Z})^\times$ est il cyclique ?

Ex.2.11 📌 *(Interrogation oct19)* Montrer qu'on a $\varphi(315) = 144$. Que vaut $4^{144}\ [315]$? $4^{145}\ [315]$?
Montrer qu'on a $5^{145} = 5\ [315]$. Que vaut $5^{144}\ [315]$?

Homothéties de $\mathbb{Z}$/n$\mathbb{Z}^\times$ (RSA)

Ex. 3.1. ✍⬚ Soit A un groupe abélien et soit n le maximum des ordres des éléments de A.
a. Observer que l'application $\phi : \mathbb{Z} \to \mathrm{End}(A)$, $\lambda \mapsto (a \mapsto \lambda a)$ est un homomorphisme d'anneaux. Quel est son noyau ?
b. Montrer que ϕ induit un isomorphisme du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$ sur le groupe des homothéties bijectives de A.
Quel est ce groupe pour $A = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

Ex.3.2. ✍⬚ **a.** Soit p un nombre premier. Pour quelles valeurs de $e \in \mathbb{Z}$ l'application entre ensembles $h_e : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $x \mapsto x^e$ est elle une bijection ?
Peut on donner une expression algébrique de l'application réciproque ? (Utiliser le théorème d'Euler-Fermat.)
Exemple : $p = 37$, $e = 5$: calculer $h_e^{-1}(10)$.
b. Soient $p_1, \ldots, p_k$ des nombres premiers distincts et $e \in \mathbb{Z}$. On note n le produit $p_1 \cdots p_k$ et h l'application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto x^e$. L'application h est elle un homomorphisme d'anneaux ?
Montrer soigneusement que l'application h est bijective si et seulement si pour chaque $i \in \{1, \ldots, k\}$ l'application $x \mapsto x^e$: $\mathbb{Z}/p_i\mathbb{Z} \to \mathbb{Z}/p_i\mathbb{Z}$ est bijective.
En déduire les valeurs de e pour lesquelles h est bijective. Quelle est alors l'expression de l'application réciproque ?
c. Exemple : $n = 165$, $e = 9$. Calculer $h^{-1}(10)$.
Même n, $e = 10$; calculer le noyau de la restriction de h à $(\mathbb{Z}/n\mathbb{Z})^\times$
d. L'application $\mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$, $x \mapsto x^5$ est elle bijective ?

Ex.3.3. 🌼📌⚙ On considère l'anneau $A = \mathbb{Z}/112\mathbb{Z}$ et son groupe des éléments inversibles $A^\times$.
a. A partir de quelle rang la suite $(6^n)_n$ est elle périodique ? Quelle est alors sa période ?
a. L'application $f : A^\times \circlearrowleft$, $x \mapsto x^{67}$ est elle bijective ? Si oui pouvez vous calculer $f^{-1}(3)$?
L'application $x \mapsto x^{67}$ est elle bijective sur l'anneau A entier ?
b. Les applications $x \mapsto x^7$ et $x \mapsto x^{43}$ coïncident elles sur $A^\times$? Sur A entier ?
❀ Explorer les réponses avec Sagemath par des méthodes élémentaires ou par des instructions de niveau 3 :

```
A=Zmod(112)
print(A);print(A.unit_group())
l=[A(x) for x in A.unit_group()]
print(len(l),l)
```

Ex.3.4. ✍★ Quels sont les automorphismes du groupe $(\mathbb{Z}/21\mathbb{Z})^\times$?

Ex.3.5. 📌 *(Int1 mars 2021)* **a.** Montrer que l'application $(\mathbb{Z}/11\mathbb{Z})^\times \circlearrowleft$, $x \mapsto x^3$ est un isomorphisme et donner une expression algébrique de l'application réciproque.
En déduire que l'application $\mathbb{Z}/11\mathbb{Z} \circlearrowleft$, $x \mapsto x^3$ est bijective.
Quelle est la racine cubique de 2 dans $\mathbb{Z}/11\mathbb{Z}$?
b. Montrer que l'application $(\mathbb{Z}/165\mathbb{Z})^\times \circlearrowleft$, $x \mapsto x^3$ est bijective et donner une expression algébrique de l'application réciproque.
Quel est la racine cubique de 86 dans $(\mathbb{Z}/165\mathbb{Z})^\times$?

Ex.3.6. 📌 *(int2 avril 2022)*
a. Quels sont les ordres possibles d'un éléments du groupe $(\mathbb{Z}/13\mathbb{Z})^\times$? Quel est l'ordre de 10 dans ce groupe ?
b. Identifier l'image de l'application $(\mathbb{Z}/13\mathbb{Z})^\times \circlearrowleft$, $x \mapsto x^3$
c. Montrer que l'application $(\mathbb{Z}/5\mathbb{Z})^\times \circlearrowleft$, $x \mapsto x^3$ est bijective et donner une expression algébrique de l'application réciproque.
d. Pouvez vous exhiber $x \in \mathbb{Z}/65\mathbb{Z}$ tel que $x^3 = 3$?
e. Pouvez vous exhiber $x \in \mathbb{Z}/65\mathbb{Z}$ tel que $x^3 = 5$?

TP RSA

Source : sujet de TP de Christophe Cazanave, déc. 2019, cf Cf https://math.unice.fr/~cazanave/fr/L3eff/TP/tp2.html

Instructions Sagemath en lien avec le sujet :

```
euler_phi(10)
factor(10616692275) #factor?
a=mod(2,11);print(a^10,a^(-1),a.parent())
mod?
Integer(str(mod(2,11))) #par exemple mod(2,11)%3 produit une erreur
2^(-1)%11 #bizarre, documentation sur a%b ?
(2%11)%3
2^10616692270673 %11 #↝ RuntimeError: Aborted
mod(2,11)^10616692270673 #↝ 8
e=10616692275;timeit("2^e %11") #↝ 5 loops, best of 3: 2.55 s per loop
e=10616692275;timeit("mod(2,11)^e") #↝ 625 loops, best of 3: 7.65 µs per loop
xgcd(2,10)[1]
```

Conversion chaîne de caractères ⟷ nombre entier :

```
#numcode(mot) n'est défini que pour un mot sur l'alphabet lchar.
lchar=' abcdefghijklmnopqrstuvwxyz'
len_lchar=len(lchar)
num={lchar[i]:i for i in range(len_lchar)}
def numcode(mot):
    return(sum(num[mot[i]]*len_lchar^i for i in range(len(mot))))
def decode_num(n):
    n1=n//len_lchar;c=lchar[n%len_lchar]
    if n1==0:return(c)
    else:return(c+decode_num(n1))
```

Au laboratoire de mathématiques, tous les messages que s'écrivent les chercheurs sont codés suivant le protocole suivant:

- On a choisi 3 entiers premiers p_1, p_2 et p_3 et en les multipliant on a créé un entier n. On a choisit convenablement un entier e pour obtenir une clé publique :
  `n=313297851918307610502911324433872045797703258998425302542562974 63`
  `e=10616692270673`
- Les messages alphanumériques (sur l'alphabet `lchar`) sont transformés en un entier M (comme dans le tp2) via la fonction `num_code()` donnée ci-dessus.
- L'entier M est crypté sous la forme $(M^e \bmod n)$ grâce à la clé publique de cryptage et transmis sous forme alphanumérique via la fonction `decode_num` donnée ci-dessus.

1. Transmettre de façon cryptée le message suivant: `"dans ce cours on apprend des choses utiles"`

2. Ce protocole n'est pas sûr. Vous avez intercepté un message. Décodez le, (en laissant apparents vos calculs intermédiaires)!
`message="o zdjsve rcnyjaxblt kqmsqdkvvekxlohsrfmwu rwh"`

3. Quelle est la longueur maximal d'un message (écrit avec l'alphabet `lchar` et transformé en un entier avec la fonction `numcode` donnés ci-dessus) qu'on peut crypter avec le couple (n,e) donné sans perdre le message ? Que se passe t-il si on déborde de cette limite ? (Essayez !)

Construire une clef (n,e) pour crypter le message
`"j ecris un bien long message bien que je n aie pour de vrai pas grand chose a dire"`
et tester la.

TP factorisation des entiers

Références
[M. Demazure, *cours d'algèbre*, Cassini 1997, §1.5]
[von zur Gathen, Gerhard, *Modern computer algebra*, Cambridge univ. press 1999, §19]

Que dit la documentation Sagemath sur l'instruction `factor()` ? Quel est l'algorithme utilisé ?

Algorithme naïf de factorisation d'un entier

Pour n préalablement défini :

```
d=2
while n%d!=0:d=d+1
print(d)
```

On peut être un peu moins naïf en restreignant d aux entiers $< \sqrt{n}$, en testant d'abord la primalité avec 2 puis en ne testant que les d impairs ; ou encore en testant d'abord la primalité avec $2, 3$ puis en ne testant que les d premiers avec $2, 3$ (en paramétrant de tels d).
Quel temps gagne t-on ?
Essayer avec `p=next_prime(10^6);pp=next_prime(p);n=p*pp` par exemple et en mesurant le temps comme suit :

```
import time
p=next_prime(10^7);pp=next_prime(p);n=p*pp
t=time.time()
d=3
while n%d!=0:d=d+2
tt=time.time()-t
print(d,N(tt,digits=3))
#time.strftime('%d %H %M %S', time.gmtime(int(tt)-60*60*24))
```

⇝ 10000019 9.97 sur SageMathCell[1]

Période d'une suite récurrente d'entiers modulo n

Soit X un ensemble fini et $f : X \circlearrowleft$ une application ; alors toute suite (x_n) définie par $x_0 \in X$ et la relation de récurrence $x_{k+1} = f(x_k)$ est périodique à partir d'un certain rang, de période p inférieure ou égale au cardinal de X. Les périodes de (x_n) sont les multiples de p.

Algorithme de Brent de recherche de la période (pour f et x_0 préalablement définis) :

```
i,p,x,y=(0,1,x0,f(x0))
while x!=y:
    if p<=i:i,p,x,y=(i,p+1,x,f(y))
    else:i,p,x,y=(i+p,1,y,f(y))
print(i,p)
```

Exemple : période du développement décimal d'une fraction rationnelle $\frac{a}{b}$: $X = \{0, \dots, b-1\}$, $f : x \mapsto (10x)\%b$, $x_0 = a\%b$

```
a,b=(2843,7750)
def f(x):return(10*x%b)
x0=a%b

i,p,x,y=(0,1,x0,f(x0))
while x!=y:
    if p<=i:i,p,x,y=(i,p+1,x,f(y))
    else:i,p,x,y=(i+p,1,y,f(y))
print(i,p)
```

```
#verif
print((a/b).n(digits=2*b))
```

i est le temps d'entrée dans le régime périodique ; p est la période. L'algorithme ne donne pas une valeur de i optimale mais donne une valeur optimale de p.

Valeur espérée de la période de f ? Faire le lien avec le "problème des anniversaires" : espérence du nombre de tirrage avec remise à faire parmi $\{1,\dots,n\}$ pour qu'une valeur au moins soit tirée deux fois au moins. Réponse : de l'ordre de $\sqrt{n}$.

Essayer

- avec la fonction f ci-dessus pour diverses valeurs de a, b
- avec une progression arithmétique $x \mapsto ax+b$ dans $\mathbb{Z}/n\mathbb{Z}$
- avec une progression géométrique $x \mapsto x^a$ dans $\mathbb{Z}/n\mathbb{Z}$

Algorithme rho de Pollard

On suppose $X = \mathbb{Z}/n\mathbb{Z}$ et f est compatible avec la réduction modulo les facteurs de n.
On modifie le test d'égalité $x = y$ dans l'algorithme de Brent par $\mathrm{pgcd}(x-y, n) = 1$, concrètement par `(x-y).is_unit()`. Pour f pris au hasard l'espérance de la période est de l'ordre de $\sqrt{p}$ avec p le plus petit facteur premier de n. Une telle période s'obtient plus probablement par une occurence de $\mathrm{pgcd}(x-y, n) > 1$ avec $x \neq y$, autrement dit avec $\mathrm{pgcd}(x-y, n)$ facteur non trivial de n.

Essayer avec `p=next_prime(10^7);pp=next_prime(p);n=p*pp;print(p)`
, $f(x) = x^2 + 1 \bmod n$; comparer avec l'algorithme naïf de recherche d'un facteur premier de n. Essayer avec d'autres fonctions f comme une progression arithmétique.

Puis avec le n du TP RSA :
`n=313297851918307610502911324433872045797703258998425302542562974 63`

---

1. (https://sagecell.sagemath.org/?z=eJzLzC3ILypRKMnMTeXlKrDNS60oiS8oAvI0DA3izDWtC1DECjSt82wLtAoKeLlKbEF69ECEhiYvV4qtMS9XeUZmTqpCnmqKoq2BVYptirYRUB2KQt0SoC1FmXklGik6fholJTopmemZJcW2xpqaAFlBK-w=&lang=sage&interacts=eJyLjgUAARUAuQ==) ↩

TD 6 - Polynômes - 15avr24

Version du 21 avril 24 (F-X. Dehon)
Exercices prioritaires : 1.4, 1.7d, 1.10, 1.12-13 (TP4), 3.1, 6.1e, 6.4 (TP) *Les exercices type sont marqués* 📌

📜 Notions, énoncés et méthodes

- Un polynôme $\sum_{k\geq 0} a_k X^k$ à coefficients dans un anneau commutatif $\mathbb{k}$ s'identifie à la **suite de ses coefficients** $(a_k)_{k\in\mathbb{N}}$, lesquels sont supposés nuls à partir d'un certain rang.
  Le **degré** d'un polynôme non nul est le plus grand indice de ses coefficients non nuls ; le coefficient correspondant est appelé **coefficient dominant**. Le degré du polynôme nul n'est pas défini.
- Si $\mathbb{k}$ est **intègre** alors le produit de deux polynômes non nuls est non nul, de degré la somme des degrés et de coefficient dominant le produit des coefficients dominants, de sorte que $\mathbb{k}[X]$ est lui même intègre et la fonction degré est croissante relativement à la relation de divisibilité.
- Un polynôme non nul est dit **irréductible** s'il ne peut pas s'écrire comme produit de deux polynômes qui ne sont ni l'un ni l'autre inversibles pour la multiplication.
  Lorsque $\mathbb{k}$ est intègre les seuls **polynômes inversibles pour la multiplication** sont les polynômes constants égaux à un élément inversible de $\mathbb{k}$.
- Si P, Q sont deux polynômes avec Q non nul et de coefficient dominant inversible dans $\mathbb{k}$ alors on peut expliciter des polynômes P_1 et R vérifiant $P = QP_1 + R$ et $R = 0$ ou $\deg(R) < \deg(Q)$ (**division euclidienne**).
  Cas particulier : pour $a \in \mathbb{k}$ on a toujours $P = (X - a)P_1 + P(a)$ faisant le **lien entre évaluation en a et racine**, cf ex.1.7.
- Si $\mathbb{k}$ est un corps alors $\mathbb{k}[X]$ muni de la division euclidienne est un **anneau euclidien** de sorte qu'on peut copier de l'**arithmétique** des entiers les énoncés et les calculs issus de la division euclidienne : Tout idéal est engendré par le **pgcd** d'une famille quelconque de générateurs, algorithme de calcul du pgcd et d'une **relation de Bézout** lorsque la famille est finie, calcul des solutions d'un **système d'équations linéaires** avec second membre, existence et calcul de la **forme de Smith** d'une matrice à coefficients dans $\mathbb{k}[X]$, existence et unicité (aux unités près) d'une **décomposition en facteurs irréductibles**, **théorème des restes chinois** pour l'anneau quotient $\mathbb{k}[X]/(PQ)$.
- Certains **algorithmes naïfs** sur les entiers n'ont leur correspondant dans $\mathbb{k}[X]$ que si $\mathbb{k}$ est **fini**. Ainsi il n'est pas clair a priori qu'on puisse décider de l'irréductibilité ou calculer une factorisation d'un polynôme de $\mathbb{Q}[X]$. (Cela le sera a posteriori.)
- Méthodes spécifiques : L'anneau $\mathbb{k}[X]$ et ses quotients $\mathbb{k}[X]/(P)$ ont une structure de $\mathbb{k}$**-espace vectoriel**, de dimension finie pour le second.
  Notion d'**évaluation** et de **racines**, polynômes irréductibles de degré 1. (Est-ce vraiment spécifique ?)
  Notion de **polynôme dérivé**, formule de Taylor
  Comparaison de la factorisation dans $\mathbb{Z}[X]$, $\mathbb{Z}/p[X]$, $\mathbb{Q}[X]$ et $\mathbb{C}[X]$.

❀ **Implémentation d'algorithmes et expérimentations avec Sagemath**.

- On déclare dans Sagemath la variable X de l'anneau $\mathbb{Q}[X]$ par l'instruction `X=QQ['X'].gen()` ; toute combinaison linéaire de puissances de X sera alors de type $\mathbb{Q}[X]$. Essayer `X=QQ['X'].gen();print((X^2+1).parent())`. On peut choisir un autre nom que X : `XX=QQ['XX'].gen();print((1+XX)^2)`.
  On aura également affaire aux anneaux de polynômes $\mathbb{Z}[X]$, $\mathbb{F}_p[X]$ qui s'obtiennent dans Sagemath en remplaçant `QQ` par `ZZ` et `GF(p)`, p nombre premier explicite ou bien variable ayant déjà comme affectation un nombre premier.
- On dispose comme avec le type `ZZ` des instructions `P%Q`, `gcd(P,Q)`, `xgcd(P,Q)`.
- Un polynôme peut être évalué comme une fonction `P(2)`, `P(Q)` et dérivé `P.derivative()`
- La liste des coefficients d'un polynôme s'obtient par `P.list()` ; inversement on peut construire le polynôme P dont la liste des coefficients est l par `QQ['X'](l)` : essayer `QQ['X']([2,0,1,3])`.
- On déclare la variable, disons x, égale à la classe de X dans l'anneau quotient $\mathbb{Q}[X]/(P)$, pour P un polynôme explicitement donné, par l'instruction `x=QQ['X'].quotient(P).gen()`. Essayer `X=QQ['X'].gen();x=QQ['X'].quotient(X^2+1).gen();print(x^2)`.
  Les coordonnées de la classe d'un polynôme Q dans l'anneau quotient $\mathbb{Q}[X]/(P)$ relativement à la base $(1, \bar{X}, \ldots, \bar{X}^{\deg(P)-1})$ s'obtiennent par l'instruction `Q(x).list()`.

Les **expérimentations** concistent le plus souvent à tester si un polynôme donné est irréductible, à calculer une factorisation ou encore à déterminer un polynôme annulateur ou le polynôme minimal d'un nombre algébrique, à tester si un tel nombre est nul.

Comme on peut s'y attendre ces questions ont déjà leurs réponses dans Sagemath : `P.is_irreducible()`, `factor(P)`, `X=QQ['X'].gen();QQ['X'].quotient(X^2+1).is_field()` `z.minpoly()`, `bool(z==0)` ; ce sont des instructions de niveau 3 (on n'en connaît pas la méthode, elles donnent une réponse tirée du chapeau) qu'on peut utiliser par curiosité mais qui ne répondent pas à notre objectif.

Arithmétique élémentaire, révisions de L1-L2

Ex.1.1 📌 Soient $P = X^4 + 2X + 1$ et $Q = 2X^2 + X + 2$ deux polynômes de $\mathbb{Z}[X]$.
a. Calculer le reste de la division euclidienne de P par Q puis le pgcd de P et Q dans $\mathbb{F}_3[X]$ et dans $\mathbb{F}_5[X]$.
Quel lien peut on faire entre le pgcd de P et Q dans $\mathbb{F}_5[X]$ et le pgcd dans $\mathbb{Z}[X]$?
b. Calculer une relation de Bézout entre P et Q dans $\mathbb{F}_5[X]$ et dans $\mathbb{Q}[X]$.
Y a t-il un lien entre ces deux relations ? Y a t-il une relation de Bezout entre P et Q dans $\mathbb{Z}[X]$?
❀Exemples de calculs avec Sagemath↗
c. ✍️📓 Soient $\Bbbk$ un corps (commutatif) et $P, Q \in \Bbbk[X]$. Démontrer que P et Q sont premiers entre eux si et seulement si leur ppcm est PQ.

Ex.1.2. 📌 *Récurrence linéaire* - Pour $n \geq 0$ on écrit $a_n X + b_n$ le reste de la division euclidienne de X^n par $X^2 + 3X + 3$ dans $\mathbb{Q}[X]$.
a. Montrer que le couple (a_n, b_n) est déterminé par (a_0, b_0) et une relation de récurrence à expliciter. Observer que a_n et b_n sont entiers quel que soit n.
b. Calculer efficacement les entiers a_{17}, b_{17}. Explicitez votre (vos) stratégie(s).
c. Soit $M = \begin{pmatrix} 0 & -3 \\ 1 & -3 \end{pmatrix}$. Observer que le polynôme minimal de M est $P = X^2 + 3X + 3$ puis que M^n coïncide avec $(X^n \% P)(M)$. Cela donne t-il une façon efficace de calculer M^{17} par exemple ?

Ex.1.3 ✍️📓 *Polynômes irréductibles* - Soit $\Bbbk$ un corps commutatif.
a. Observer que les polynômes inversibles pour la multiplication dans $\Bbbk[X]$ (les unités de $\Bbbk[X]$) sont exactement les polynômes non nuls de degré 0.
Quels sont les polynômes inversibles de $\mathbb{Z}[X]$? Et ceux de $\mathbb{Z}/4\mathbb{Z}[X]$?
b. Montrer par récurrence (tautologique) sur le degré que tout polynôme non nul s'écrit comme le produit d'une unité et d'une famille finie de polynômes irréductibles de coefficient dominant 1.
c. Soit $\mathcal{P}$ l'ensemble des polynômes irréductibles de $\Bbbk[X]$ de coefficients dominant 1. Montrer que tout polynôme non nul s'écrit de manière unique à l'ordre près comme produit d'une unité et d'une famille finie d'éléments de $\mathcal{P}$. Par quel objet peut on représenter une telle factorisation ?
d. Déterminer la liste des polynômes irréductibles de degré ≤ 4 de $\mathbb{F}_2[X]$.
e. 📌 Calculer par une méthode élémentaire une décomposition en facteurs irréductibles du polynôme $X^3 + 9X^2 + 17X + 21$ dans $\mathbb{Z}[X]$ et dans $\mathbb{F}_2[X]$.

Ex.1.4. ✍️📓 **a.** Soit $\Bbbk$ un corps (commutatif) et P un polynôme à coefficients dans $\Bbbk$. Montrer l'équivalence entre
(i) P est irréductible dans $\Bbbk[X]$.
(ii) $\Bbbk[X]/(P)$ est un corps.
b. Les anneaux suivants sont ils des corps ? $\mathbb{R}[X]/(X^2+1)$, $\mathbb{C}[X]/(X^2+1)$, $\mathbb{Z}[X]/(X^2+1)$, $\mathbb{F}_2[X]/(X^2+1)$.
c. 📌 *(Session 2 2022)* Donner un exemple de corps de la forme $\mathbb{F}_3[X]/(P)$ de cardinal 9. Justifiez.

Ex.1.7. ✍️📓 *Racines et factorisation* - Soient $\Bbbk$ un anneau commutatif, $a \in \Bbbk$ et $P \in \Bbbk[X]$.
a. Observer que P s'écrit $(X-a)Q + P(a)$ pour un $Q \in \Bbbk[X]$ et en déduire que a est racine de P si et seulement si $X - a$ divise P dans $\Bbbk[X]$.
Observer que l'application "Evaluation en a" : $\Bbbk[X] \to \Bbbk$, $P \mapsto P(a)$ induit un isomorphisme $\Bbbk[X]/(X-a) \to \Bbbk$. Cf la notion de *factorisation canonique*.
b. On suppose $\Bbbk$ intègre et P non nul. Montrer que P a au plus $\deg(P)$ racines (cf f5-ex2.5a). Quelle factorisation de P obtient on ?
c. Que se passe t-il si on ne suppose pas $\Bbbk$ intègre ?
Exemples : 1. Quelles sont les factorisations de $X^2 - 1$ dans $(\mathbb{Z}/8\mathbb{Z})[X]$?
2. Observer que $X^3 - 1$ a exactement trois racines dans $\mathbb{Z}/9\mathbb{Z}$, que les monômes $X-1$, $X-4$, $X+2$ divise X^3-1 mais pas le produit de deux d'entre eux.
d. 📌 On suppose $\Bbbk = \mathbb{Z}$ et P de degré ≥ 1. Soient a, b deux entiers avec $b \neq 0$ et $a \wedge b = 1$. Montrer que si $\frac{a}{b}$ est racine de P dans $\mathbb{Q}$ alors le coefficient dominant de P est un multiple entier de b, le coefficient constant de P est un multiple entier de a et $bX - a$ divise P dans $\mathbb{Z}[X]$ (Faites une récurrence sur le degré de P).

En déduire que si P est de coefficient dominant 1 alors toute racine rationnelle de P est entière.
❀ Quel algorithme en déduit on pour la recherche des racines dans $\mathbb{Q}$ d'un polynôme de $\mathbb{Q}[X]$?
Exemple : $P = 2X^3 + 3X^2 + 7X + 3$. Quelles sont les racines rationnelles de P ? Quelle factorisation de P obtient on dans $\mathbb{Z}[X]$?

Ex.ex1.10. ✍️🗒️ Soient $\mathbb{k}$ un corps (commutatif) et P un polynôme à coefficients dans $\mathbb{k}$ de degré 2 ou 3. Montrer que P est irréductible dans $\mathbb{k}[X]$ si et seulement si P est sans racine dans $\mathbb{k}$.
L'énoncé est il vrai sans condition sur le degré ?
L'énoncé est il vrai dans $\mathbb{Z}[X]$? Voir l'ex. 1.7d.
Exemple : le polynôme $3X^3 + X^2 + 1$ est il irréductible dans $\mathbb{F}_2[X]$? Et dans $\mathbb{Q}[X]$?

Ex.1.8. ✍️🗒️ *Racines multiples*
a. Soit P un polynôme de $\mathbb{Q}[X]$ de degré ≥ 1 et $a \in \mathbb{Q}$. Montrer que $(X-a)^k$ divise P dans $\mathbb{Q}[X]$ si et seulement si $P(a) = P'(a) = \ldots = P^{(k-1)}(a) = 0$
b. Plus généralement montrer l'équivalence entre
(i) $\exists Q \text{ de degré } \geq 1,\ Q^2 \mid P$.
(ii) $P \wedge P'$ est de degré ≥ 1.
c. Les énoncés (a) et (b) ont ils des analogues dans $\mathbb{F}_p[X]$? Cf ex.6.2

Ex.1.9. Montrer que tout polynôme $\mathbb{R}[X]$ de degré impair admet une racine dans $\mathbb{R}$.
❀ Pouvez vous construire un algorithme donnant le développement décimal d'une racine réelle de $X^5 + X + 1$?

Ex.1.12. ✍️🗒️ *Interpolation de Lagrange[1] et théorème des restes chinois*
a. Soit $\mathbb{k}$ un corps (plus généralement un anneau intègre), a, b deux éléments distincts de $\mathbb{k}$ et $k, l \geq 1$ deux entiers. Montrer que les polynômes $(X-a)^k$ et $(X-b)^l$ sont premiers entre eux. Pouvez vous exhiber une relation de Bézout ?
b. Soient $a_1, \ldots, a_n$ des éléments distincts de $\mathbb{k}$.
Observer que l'application $\mathbb{k}[X]/(X-a_i) \to \mathbb{k}$, $P \mapsto P(a_i)$ est un isomorphisme d'anneaux.
En déduire que l'application $\Phi : \mathbb{k}[X]/\prod_i (X-a_i) \to \prod_i \mathbb{k}$, $P \mapsto (P(a_1), \ldots, P(a_n))$ est un isomorphisme d'anneaux.
Que se passe t-il si les a_i ne sont pas tous distincts ?
c. Pouvez vous exhiber le représentant de degré $< n$ de l'antécédent de $(b_1, \ldots, b_n)$ par Φ ?

Ex.1.13. 🍇 *Algorithme de Kronecker*[1:1] Soient $P, Q \in \mathbb{Z}[X]$, $n \geq 1$ et $a_1, \ldots, a_n \in \mathbb{Z}$.
a. Observer que si P divise Q dans $\mathbb{Z}[X]$ alors $P(a_i)$ divise $Q(a_i)$ dans $\mathbb{Z}$. En déduire avec l'exercice 1.12 un algorithme de recherche des facteurs de Q dans $\mathbb{Z}[X]$. (Pour diminuer le nombre de calculs observer qu'on peut imposer $P(a_1) > 0$ si $P(a_1) \neq 0$.)
❀ Implémenter cet algorithme avec Sagemath.
b. Montrer de la sorte que $X^2 - 2$ est irréductible dans $\mathbb{Z}[X]$. (Certains choix de la famille (a_i) sont plus judicieux que d'autre).
Le polynôme $6X^2 - 7X - 3$ est il factorisable dans $\mathbb{Z}[X]$?
Qu'en est il de $X^4 + 1$? Utiliser Sagemath au besoin.

Factorisation comparée dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$

Ex.2.1 ✍️🗒️ Pour $P \in \mathbb{Z}[X]$ on note $c(P)$ ("le contenu de P") le pgcd des coefficients de P.
Pour $P \in \mathbb{Q}[X]$ on définit $c(P)$ comme le nombre $\frac{1}{d}c(dP)$ où d est tel que dP est à coefficient entier.
a. Vérifier que $\frac{1}{d}c(dP)$ ne dépend pas du choix de d.
Montrer que pour tout $P \in \mathbb{Q}[X]$, P est à coefficients entiers si et seulement si $c(P)$ est entier. En particulier $\frac{1}{c(P)}P \in \mathbb{Z}[X]$.
b. Montrer que pour $P, Q \in \mathbb{Z}[X]$ on a $c(PQ) = c(P)c(Q)$.
Indication : Observer d'abord $c(P)c(Q) \mid c(PQ)$ dans $\mathbb{Z}$. Observer ensuite que si p est un facteur premier de $c(PQ)$ alors PQ=0 dans $\mathbb{F}_p[X]$ donc $P = 0$ ou $Q = 0$ dans $\mathbb{F}_p[X]$.
c. Soient $P, Q \in \mathbb{Z}[X]$. Montrer que P divise Q dans $\mathbb{Z}[X]$ si et seulement si $c(P)$ divise $c(Q)$ dans $\mathbb{Z}$ et si P divise Q dans $\mathbb{Q}[X]$.
En déduire que P est irréductible dans $\mathbb{Z}[X]$ si et seulement si $c(P) = 1$ et P est irréductible dans $\mathbb{Q}[X]$.
En déduire que le pgcd de P et Q dans $\mathbb{Z}[X]$ coïncide avec le pgcd de P et Q dans $\mathbb{Q}[X]$. Obtient on ainsi une relation de Bezout entre P et Q dans $\mathbb{Z}[X]$?
d. Exemple : Montrer que $X^3 + 2X + 1$ est irréductible dans $\mathbb{Q}[X]$.
Déterminer la décomposition en facteurs irréductibles de $1 + X + X^2 + \ldots + X^5$ dans $\mathbb{Q}[X]$. (Il y a ici la possibilité d'une observation ad-hoc qui conduit au résultat bien plus rapidement que la méthode générique !)

Ex.2.2. ✍️🗒️ *Cf ex.1.7.* **a.** Soient p, q deux entiers non nuls premiers entre eux et $P \in \mathbb{Z}[X]$. Observer avec l'exercice 2.1 que $qX - p$ divise P dans $\mathbb{Z}[X]$ si et seulement si il divise P dans $\mathbb{Q}[X]$.
Le polynôme $qX - p$ admet il une racine entière ?
b. Observer que $X^2 - 2$ est irréductible dans $\mathbb{Z}[X]$. En déduire que $\sqrt{2} \in \mathbb{R}$ est irrationnel.
Peut on montrer de la même façon que le nombre $\sqrt{2} + \sqrt{3}$ est irrationnel ? Voir l'ex. 5.4.

Factorisation comparée dans $\mathbb{Z}[X]$ et dans $\mathbb{F}_p[X]$

"**Ex.3.1** 📌 **a.** ✍️🗒️ Soit $P \in \mathbb{Z}[X]$ de contenu 1 (cf. ex.2.1.) et p un nombre premier qui ne divise pas le coefficient dominant de P. Montrer que si P est irréductible dans $\mathbb{F}_p[X]$ alors P est irréductible dans $\mathbb{Z}[X]$.
La réciproque est elle vraie ?
b. Montrer que $1 + X + X^2 + X^3 + X^4$ est irréductible dans $\mathbb{Z}[X]$.
c. Le polynôme $X^3 - 2X + 2$ est il irréductible dans $\mathbb{F}_3[X]$? dans $\mathbb{F}_5[X]$? dans $\mathbb{Z}[X]$?

Ex.3.1.bis. ✍️ *Critère d'Eisenstein*[1:2]
a. Soient $P \in \mathbb{Z}[X]$ unitaire (*i.e.* de coefficient dominant 1) de degré n et p un nombre premier. On suppose d'une part $P(0) = pq$ avec $p \wedge q = 1$, d'autre part $P = X^n$ dans $\mathbb{F}_p[X]$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.
b. En déduire l'existence de polynôme irréductible de tout degré dans $\mathbb{Z}[X]$.
c. Exemple : Montrer que $(X+1)^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ en calculant $(X+1)^4 + 1$ dans $\mathbb{F}_2[X]$? (Utiliser l'homomorphisme de Frobenius (ex.6.1) pour répondre sans calcul).
Observer pour $P \in \Bbbk[X]$ l'équivalence entre P est irréductible et $P(X+1)$ est irréductible.

Ex.3.2 ✍️ Soit $p \geq 2$ un nombre premier. Montrer avec le théorème d'Euler-Fermat que le polynôme $X^p - X$ est scindé à racines simples (c'est à dire de multiplicité 1) dans $\mathbb{F}_p[X]$. Qu'en est il dans $\mathbb{Z}[X]$?

Ex.3.3. 📌 Le nombre -1 est il un carré dans $\mathbb{F}_7$?
A quelle condition sur le nombre premier p le nombre -1 est un carré dans $\mathbb{F}_p$? Exhiber trois tels p.
Exhiber un p tel que -1 soit une puissance 4-ème dans $\mathbb{F}_p$. Quelles sont alors les racines de $X^4 + 1$ dans $\mathbb{F}_p$?
Indication : exploiter le fait que le groupe multiplicatif $\mathbb{F}_p^\times$ est cyclique et observer que -1 est le seul élément d'ordre 2 lorsque $p > 2$

Ex.3.4. 📌🍇 *Irréductibilité de $X^4 + 1$.*
a. Observer l'égalité

$$X^4 + 1 = (X^2 + i)(X^2 - i) \quad (*)$$

dans $\mathbb{C}[X]$ selon l'identité remarquable $a^2 - b^2 = (a+b)(a-b)$. En déduire la décomposition en facteurs premiers dans $\mathbb{C}[X]$ puis la décomposition

$$X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) \quad (**)$$

dans $\mathbb{R}[X]$.
b. Observer que -1 est le seul élément d'ordre 2 dans $\mathbb{F}_p^\times$ puis que tout élément de $\mathbb{F}_p^\times$ d'ordre 4 est de carré -1 dans $\mathbb{F}_p$.
En déduire que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1\ [4]$.
En déduire que la factorisation $(*)$ se réalise dans $\mathbb{F}_5$ mais pas dans $\mathbb{F}_7$ ni dans $\mathbb{F}_3$.
Observer que 2 est d'ordre 3 dans $\mathbb{F}_7^\times$ et que si $p \equiv 1\ [6]$ alors tout élément d'ordre 3 dans $\mathbb{F}_p^\times$ est un carré dans $\mathbb{F}_p$.
En déduire que la factorisation $(**)$ se réalise dans $\mathbb{F}_7$. Se réalise t-elle dans $\mathbb{F}_3$?
c. Montrer que $X^4 + 1$ admet une racine dans $\mathbb{F}_p$ si et seulement si $p = 2$ ou $p \equiv 1\ [8]$.

d. *Approche élémentaire* Chercher une décomposition de la forme $(X^2 + aX + b)(X^2 - aX + 1/b)$ (Pourquoi cette forme ?).
Observer qu'une telle factorisation existe dans $\Bbbk[X]$ avec $\Bbbk$ intègre ssi l'un des nombres $-1, 2, -2$ est un carré dans $\Bbbk$.*
- Factorisation sortie du chapeau :
Observer $X^4 + 1 = (X^2)^2 - (-1) = (X^2+1)^2 - 2X^2 = (X^2 - 1) - (-2)X^2$ et on sait $a^2 - b^2 = (a+b)(a-b)$.
e. Montrer que l'un des nombres $-1, 2, -2$ est toujours un carré dans $\mathbb{F}_p$ pour $p > 2$.
Indication : Notons H l'ensemble des carrés des éléments de $\mathbb{F}_p^\times$. Observer que H est un sous-groupe de $\mathbb{F}_p^\times$ et que le groupe quotient $\mathbb{F}_p^\times / H$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +)$.
❀ Expérimentation naïve avec Sagemath↗

f. Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$. *(voir les ex.1.13 et 3.1bis)*
Que dire de l'énoncé «Soit P un polynôme unitaire à coefficients entiers ; alors P est irréductible dans $\mathbb{Z}[X]$ ssi il l'est dans $\mathbb{F}_p[X]$ pour au moins un nombre premier p.»

Nombres complexes algébriques, sous corps de $\mathbb{C}$

Ex.5.1 ✍️📄 Soient $\Bbbk$ un corps (commutatif) et K une $\Bbbk$-algèbre commutative intègre de dimension finie comme $\Bbbk$-espace vectoriel.
a. Montrer que K est un corps.
Indication : Soit $0 \neq y \in K$. Observer que l'application $K \to K$, $x \mapsto yx$ est $\Bbbk$-linéaire et étudier sa bijectivité.
On suppose désormais que $\Bbbk$ est le plus petit sous-corps de K contenant 1.
b. Montrer que si 1 est d'ordre fini dans le groupe additif $(\Bbbk, +)$ alors 1 est d'ordre premier p et $\Bbbk$ est isomorphe à $\mathbb{F}_p$. A quoi ressemble alors le groupe additif $(K, +)$? Et le groupe multiplicatif $(K^\times, \times)$?
c. Montrer que si 1 n'est pas d'ordre fini alors $\Bbbk$ est isomorphe à $\mathbb{Q}$.
★★Montrer que K est isomorphe à un sous-corps de $\mathbb{C}$.

Ex.5.2 ✍️📄 *Rq : Le point (a) ci-dessous vaut tel quel en remplaçant $\mathbb{Q}$ et $\mathbb{C}$ par un corps commutatif $\Bbbk$ quelconque et une $\Bbbk$-algèbre K commutative intègre.*
On dit qu'un nombre complexe $z \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ s'il existe $P \in \mathbb{Q}[X]$ non nul tel que $P(z) = 0$ dans $\mathbb{C}$.
a. Montrer l'équivalence entre les conditions suivantes :
(i) z est algébrique sur $\mathbb{Q}$
(ii) la famille $(z^k)_{k\in\mathbb{N}}$ est liée sur $\mathbb{Q}$.
(iii) L'homomorphisme d'anneaux $\mathbb{Q}[X] \to \mathbb{C}$, $P \mapsto P(z)$ n'est pas injectif.
(iv) le sous-anneau $\mathbb{Q}[z] \subset \mathbb{C}$ engendré par $\mathbb{Q}$ et z est de dimension finie comme $\mathbb{Q}$-espace vectoriel.
(v) $z = 0$ ou bien il existe $P \in \mathbb{Q}[X]$ tel que $z^{-1} = P(z)$.
(vi) le sous-anneau $\mathbb{Q}[z] \subset \mathbb{C}$ engendré par $\mathbb{Q}$ et z est un corps.
b. Déduire de (a) que si $z \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ alors il en est de même de $F(z)$ pour toute fraction rationnelle $F \in \mathbb{Q}(X)$ dont z n'est pas un pôle.
Observer que $(F(z))^n$, $n \geq 0$, s'exprime comme combinaison linéaire des $z^k, 0 \leq k \leq \dim_{\mathbb{Q}}\mathbb{Q}[z] - 1$. En déduire une stratégie pour expliciter un polynôme annulateur de $F(z)$. Voir les ex.5.3-4.
c. Observer que le polynôme minimal d'un nombre complexe algébrique est irréductible. Cf ex.1.4
Quelles sont les matrices $M \in \mathrm{M}_2(\mathbb{R})$ dont le polynôme minimal dans $\mathbb{R}[X]$ est irréductible ?
d. ★★ Existe t-il des nombres complexes non algébriques sur $\mathbb{Q}$? Pouvez vous en expliciter un (avec preuve !) ?
e. Montrer que l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$ de cardinal dénombrable.

Ex.5.3 📌 **a.** Quelle est la dimension de $\mathbb{Q}[\exp(\frac{2i\pi}{5})] \subset \mathbb{C}$ comme $\mathbb{Q}$-espace vectoriel ?
Indication : expliciter un polynôme de $\mathbb{Q}[X]$ annulateur de $\exp(\frac{2i\pi}{5})$ puis déterminer les facteurs irréductibles de ce polynôme.
b. Soit $z = \mathrm{e}^{\frac{2i\pi}{6}} - 2\mathrm{e}^{\frac{4i\pi}{6}}$. Observer que les puissances de z sont toutes combinaisons linéaires à coefficients entiers des nombres $\mathrm{e}^{\frac{2ki\pi}{6}}, 0 \leq k \leq 5$. En déduire un polynôme de $\mathbb{Q}[X]$ annulateur de z. Est il minimal ?
c. Déterminer la dimension sur $\mathbb{Q}$ de $\mathbb{Q}[\exp(\frac{2i\pi}{6})]$.
d. Montrer que le nombre $z = \exp(\frac{2i\pi}{5}) + \exp(-\frac{2i\pi}{5})$ est algébrique sur $\mathbb{Q}$. Quelle est la dimension de $\mathbb{Q}[z]$ comme $\mathbb{Q}$-espace vectoriel ?
❀ Voir le TP4 "Nombres complexes algébriques"

Ex.5.4 🍇 *(cf TP4)* **a.** Trouver un polynôme annulateur à coefficients rationnels du nombre $\sqrt{2} + \sqrt{3} \in \mathbb{R}$. Est ce le polynôme minimal ?
Méthode : chercher une relation non triviale à coefficients rationnels entre les premières puissances de $\sqrt{2} + \sqrt{3}$, éventuellement en terme de relation entre leurs vecteurs de coordonnées relativement à la "base" $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$. Pourquoi trouve t-on forcément une relation non triviale ?
Alternative : Que donne le polynôme caractéristique de la matrice de l'application $x \mapsto (\sqrt{2} + \sqrt{3})x$ relativement à la $\mathbb{Q}$-"base" $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$?
b. Observer que le polynôme minimal de $\sqrt{2} + \sqrt{3}$ ne distingue pas le signe de $\sqrt{2}$ ni de $\sqrt{3}$. En déduire l'expression de ses quatre racines.
❀ Avec Sagemath on peut déclarer `z=sqrt(2)+sqrt(3)`, calculer les puissances de z, les développer par l'instruction `expand()` et entrer à la main la matrice M des coordonnées. Après enquête approfondie on s'apperçoit que les instructions suivantes rendent la liste des coefficients voulus d'une expression polynomiale explicite $P(z)$ en z :

```
P(z)=z^3
z=sqrt(2)+sqrt(3)
b=[sqrt(2),sqrt(3),sqrt(6)]
w=SR.wild(0)
zz=P(z).expand().maxima_methods().rootscontract()
```

```
l=[zz.subs(w==0)]+[zz.coefficient(i) for i in b]
print(l)
```

On construit une liste l des coordonnées des premières puissances de z qu'on convertit en matrice à coefficient dans $\mathbb{Q}$ avec l'instruction `matrix(QQ,l)`. On détermine une relation non triviale entre les colonnes de M avec la forme de Smith de M : `M.smith_form()`.

★Montrer que la famille $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est libre sur $\mathbb{Q}$.

Indication : Montrer que le polynôme X^2-2 est irréductible sur $\mathbb{Q}$ de sorte qu'on a un isomorphisme de $\mathbb{Q}$-algèbres $\mathbb{Q}[X]/(X^2-2) \xrightarrow{\simeq} \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ tel que $(1, \sqrt{2})$ est l'image de la $\mathbb{Q}$-base canonique $(1, X)$ de $\mathbb{Q}[X]/(X^2-2)$.
Montrer ensuite que le polynôme X^2-3 est irréductible dans l'anneau de polynômes $\mathbb{Q}[\sqrt{2}][X]$ et conclure de même.
Alternative plus accessible : le polynôme annulateur de $\sqrt{2}+\sqrt{3}$ trouvé plus haut est il irréductible dans $\mathbb{Q}[X]$? Qu'en déduit on ?

🆕 Nouvelles choses :

Ex.5.5 Donner une expression par radicaux des parties réelles et imaginaires des deux racines carrés du nombre complexe $1+i$.
En déduire une expression par radicaux des racines dans $\mathbb{C}$ du polynôme $X^2+2iX-\frac{5}{4}-i$
❀ Avec Sagemath : `solve([x^2+2*I*x-5/4-I],x)`. La réponse est à mi-chemin.

Ex.5.6 🍇 *Ce que résoudre une équation veut dire — Formules de Viète[1:3] pour les racines d'un polynôme de degré 3*
$a, b \neq 0$ sont deux nombres réels fixés.
a. L'application $\mathbb{C} \to \mathbb{C}$, $x \mapsto x - \frac{a}{3x}$ est elle bijective ? A défaut quelle est son image et quels sont les antécédents d'un élément donné de l'image ?
b. Soit $P = X^3 + aX + b$. Observer la forme de $P(x - \frac{a}{3x})$. En déduire une expression par radicaux des racines de P.
c. A quelle condition sur $a, b \in \mathbb{R}$ le polynôme P admet il une seule racine réelle ? Quelle est alors l'expression de cette racine ?
d. Exemple $P = X^3 + X - 1$. Donner l'expression par radicaux de la racine réelle de P.
⚙ Comment peut on prouver que cette racine n'est pas dans $\mathbb{Q}$? Que les autres racines de P ne sont pas réelles ?
⚙ Pouvez vous expliciter un vecteur directeur d'une droite de $\mathbb{R}^3$ stable par l'endomorphisme de matrice $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$?
e. Exemple $P = X^3 + X - 1$. Exprimer par radicaux les trois racines de P.
★⚙ Peut on prouver algébriquement que ces racines sont réelles (*i.e.* chacune est égale à son conjugué dans $\mathbb{C}$) ?
❀ Calculs avec Sagemath :

```
A=matrix(QQ,3,3,[0,0,1,1,0,-1,0,1,0])
P=A.charpoly()
sp = LatexExpr('~')
show(P,sp,P.parent(),sp,P.is_irreducible())
show(matrix(QQbar,A).diagonalization())
```

Factorisation dans $\mathbb{F}_p[X]$: algorithme de Berlekamp, corps finis

Ex.6.0 ✍🗒 *Petit théorème de Fermat[1:4] et homomorphisme de Frobenius[1:5].* On fixe un nombre premier p et on considère un anneau A dont $\mathbb{F}_p$ est un sous-anneau (*i.e.* A est une $\mathbb{F}_p$-*algèbre*, cf ex.5.1 ci-dessus).
a. *Formule du binome de Newton[1:6]* Montrer que le coefficient binomial $\binom{p}{k}$ est un multiple entier de p pour tout $k \in \{1, \ldots, p-1\}$. (Utiliser l'unicité de la décomposition en facteurs premiers dans $\mathbb{Q}$.)
En déduire que pour tout couple (x, y) d'éléments de A tel que $xy = yx$ on a $(x+y)^p = x^p + y^p$.
En déduire par récurrence sur $k \in \{0, \ldots, p-1\}$ qu'on a $\bar{k}^p = \bar{k}$ dans $\mathbb{F}_p$ (*Petit théorème de Fermat*).
Pour quels entiers n a t-on $\forall x \in \mathbb{Z},\ x^n \equiv x \bmod n$?
b. En déduire que si l'anneau A est commutatif l'application $A \to A$, $x \mapsto x^p$ (*homomorphisme de Frobenius*) est un homomorphisme d'anneaux $\mathbb{F}_p$-linéaire. (*i.e.* un homomorphisme de $\mathbb{F}_p$-algèbres.)
c. *Chemin inverse* Observer le petit théorème de Fermat à la lumière du théorème de Lagrange : $x^p = x$ pour tout $x \in \mathbb{F}_p$. Cf f5-ex.1.1. En déduire qu'on a $(x+y)^p = x^p + y^p$ pour tous $x, y \in \mathbb{F}_p$.
En déduire que pour $y \in \mathbb{F}_p$ fixé les fonctions polynomiales $\mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto (x+y)^p$ et $x \mapsto x^p + y^p$ coïncident, puis que les polynômes $(X+y)^p$ et $X^p + y^p$ de $\mathbb{F}_p[X]$ coïncident.
En déduire que les fonctions polynomiales $\mathbb{F}_p[X] \to \mathbb{F}_p[X]$, $y \mapsto (X+y)^p$ et $y \mapsto X^p + y^p$ coïncident sur $\mathbb{F}_p \subset \mathbb{F}_p[X]$, puis que les polynômes $(X+Y)^p$ et $X^p + Y^p$ de $(\mathbb{F}_p[X])[Y]$ coïncident.
En déduire que le coefficient binomial $\binom{p}{k}$ est un multiple entier de p pour tout $k \in \{1, \ldots, p-1\}$.
En déduire également que pour tout couple (x, y) d'éléments de A tel que $xy = yx$ on a $(x+y)^p = x^p + y^p$. (Considérer l'homomorphisme d'anneaux $(\mathbb{F}_p[X])[Y] \to A$, $P(X, Y) \mapsto P(x, y)$).

Ex.6.1 ✍️📓 *Algorithme de Berlekamp*[1:7] Soit K une $\mathbb{F}_p$-algèbre commutative non réduite à $\{0\}$ (ce qui équivaut à K est un anneau commutatif et l'unité 1_K est pour l'addition d'ordre p premier).
a. Observer que l'application $F : K \to K, x \mapsto x^p$ (le "Frobenius") est un homomorphisme de $\mathbb{F}_p$-algèbres (voir "anneau" dans le glossaire) ; en particulier elle est $\mathbb{F}_p$-linéaire. Cf. ex.6.0.
b. On suppose que K est intègre ; montrer que le sous espace des points fixes de F (l'espace propre pour la valeur propre 1) est exactement le sous-anneau $<1_K> \simeq \mathbb{F}_p$, en particulier est de dimension 1 comme $\mathbb{F}_p$- espace vectoriel.
c. On suppose que K est isomorphe au produit $K_1 \times K_2$ avec K_1, K_2 des $\mathbb{F}_p$-algèbres commutatives non réduites à $\{0\}$. Observer que l'espace des points fixes de F contient $<1_{K_1}> \times <1_{K_2}>$, en particulier est de dimension au moins 2.
d. Soit $0 \neq P \in \mathbb{F}_p[X]$ et $K = \mathbb{F}_p[X]/(P)$. Observer que si P s'écrit comme produit de deux polynômes premiers entre eux alors K est isomorphe à un produit de deux anneaux. Obtient on un critère d'irréductibilité de P ?
e. 📌 Exemple $P = X^2 + X + 1$. Déterminer la dimension de l'espace des points fixes de F sur K pour $p = 2$ puis $p = 3$. Le polynôme P est il irréductible dans $\mathbb{F}_p[X]$?
❀ Faire les calculs avec Sagemath.

Ex.6.2 ✍️ *Facteurs carrés dans P* Soit P un polynôme de $\mathbb{F}_p[X]$ de degré ≥ 1.
a. Montrer que si le polynôme dérivé P' est nul alors P s'écrit $Q(X^p)$ pour un $Q \in \mathbb{F}_p[X]$. En déduire à l'aide de 5.1.a qu'on a $P = Q^p$.
b. Montrer l'équivalence entre les deux conditions suivantes :
(i) $\exists Q \text{ de degré } \geq 1,\ Q^2 \mid P$.
(ii) $P \wedge P'$ est de degré ≥ 1.

Ex.6.3 ✍️ *Critère d'irréductibilité* Déduire des deux exercices précédents une condition nécessaire et suffisante pour qu'un polynôme de $\mathbb{F}_p[X]$ soit irréductible.
❀ Programmer avec Sagemath un test d'irreductibilité sous forme d'une fonction prenant comme argument un polynôme à coefficients entiers et un nombre premier p et rendant la valeur `True` si le polynôme est irréductible dans $\mathbb{F}_p[X]$, `False` sinon.
Ecrire d'abord "sur un cahier" la stratégie adaptée à Sagemath pour un tel programme.
Rappel : dans Sagemath les coordonnées de la classe d'un polynôme Q dans l'anneau quotient $\mathbb{F}_p[X]/(P)$ relativement à la base $(1, \bar{X}, \ldots, \bar{X}^{\deg(P)-1})$ s'obtiennent par l'instruction `Q(x).list()` où x a été déclaré par l'instruction `x=GF(p)['X'].quotient(P).gen()`.

Ex.6.4. (Cf ex.3.4) *Irréductibilité de $X^4 + 1$ via Berlekamp* - On note K l'anneau quotient $\mathbb{F}_p[X]/(X^4 + 1)$ et $\bar{X}$ la classe de X dans K.
★**a.** Observer que $\bar{X}^k$ ne dépend que de k modulo 8.
❀Former avec Sagemath la matrice de l'application $F : K \to K, x \mapsto x^p$ pour les différentes valeurs de p modulo 8. Au passage quelles sont les valeurs possibles de p modulo 8 ?
Calculer la dimension de l'espace des points fixes de F (l'espace propre E_1) dans chacuns de ces cas.
b. Sagemath rend les dimensions $1, 2, 2, 2, 4$ pour $p = 2, 3, 5, 7, 1$ modulo 8. Qu'en déduit on sur le nombre de facteurs irréductibles de $X^4 + 1$ dans $\mathbb{F}_p[X]$?
Que se passe t-il pour $p = 2$?
★ Qu'en déduit on sur l'irréductibilité de $X^4 + 1$ dans $\mathbb{Z}[X]$?

Ex.6.6 📌🍇(examen de mai21) On note P le polynôme $X^5 + X^4 + 1$ de $\mathbb{F}_2[X]$ et K l'anneau quotient $\mathbb{F}_2[X]/(P)$.
a. Expliquer pourquoi l'application $\varphi : K \to K, x \mapsto x^2$ est $\mathbb{F}_2$-linéaire et calculer sa matrice relativement à une base que vous choisirez du $\mathbb{F}_2$ - espace vectoriel sous-jacent à K.
b. Quelle est la dimension de l'espace des points fixes (l'espace propre E_1) de φ ?
Qu'en déduit on sur l'irréductibilité de P ?
c. Exhiber un point fixe Q de φ qui ne soient pas un polynôme constant puis déterminer un élément $a \in \mathbb{F}_2$ tel que le pgcd de $Q + a$ avec P soit de degré ≥ 1.
d. Déduire de ce qui précède une décomposition en facteurs irréductibles de P.
e. Quel est le cardinal du groupe multiplicatif $K^\times$?
Le groupe $K^\times$ est il cyclique ?
❀ Faire les calculs avec Sagemath.

---

1. Notices Wikipedia sur Lagrange, Kronecker, Eisenstein, Viete, Fermat, Frobenius, Newton, Berlekamp ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩

TP 4 nombres algébriques - factorisation – 23avr24

F-X. Dehon - *version du 2mai24*

I. Polynôme annulateur d'un nombre algébrique

Soient $\mathbb{k}$ un anneau commutatif ($\mathbb{k}=\mathbb{Z},\mathbb{Q}$ ou $\mathbb{F}_p$) et $z,x_1,\dots,x_r$ des éléments d'une $\mathbb{k}$-algèbre K. On suppose qu'on sait exprimer toutes les puissances de z comme combinaison linéaire à coefficients dans $\mathbb{k}$ des x_i ; alors on peut construire un polynôme non nul $P\in\mathbb{k}[X]$ dont z est racine en déterminant un élément du noyau de "la" matrice des coordonnées de $z^0,z^1,\dots,z^r$ relativement à la famille génératrice (x_i).
Alternativement, si on sait pour chaque i exprimer le produit $z\cdot x_i$ comme combinaison linéaire à coefficients dans $\mathbb{Q}$ de $x_1,\dots,x_r$ alors on peut prendre pour P le polynôme caractéristique de "la" matrice de l'application $x\mapsto zx$ relativement à la famille génératrice (x_i).

Typiquement K est un modèle de la forme $\mathbb{k}[X]/(Q)$ d'un anneau concret A, par exemple $K=\mathbb{Q}[X]/(X^9+1)$ pour l'ensemble A des nombres complexes de la forme $P(\exp(\frac{i\pi}{9}))$, $P\in\mathbb{Q}[X]$, mais ce pourrait aussi être un modèle plus compliqué comme $\mathbb{Q}[X,Y]/(Q_1(X),Q_2(Y))$ ou $\big(\mathbb{Q}[X]/Q_1(X)\big)[Y]/(Q_2(X,Y))$.
Supposons que $\mathbb{k}$ est un corps (commutatif). Dans le cas $K=\mathbb{k}[X]/(Q)$, la famille $(1,\bar X,\dots,\bar X^{\deg(Q)-1})$ est une base de K comme $\mathbb{k}$-espace vectoriel, dite canonique.
Dans le cas plus intriqué
$K=\big(\mathbb{k}[X]/(Q_1(X))\big)[Y]/(Q_2(X,Y))=\mathbb{k}[X,Y]/(Q_1(X),Q_2(X,Y))$ une base est donnée par la famille $(\bar X^i\bar Y^j)_{0\le i\le\deg(Q_1),0\le j\le\deg(Q_2)}$.

I.A. Polynôme annulateur de $\cos(\pi/9)$

Les nombres $\exp(-\frac{i\pi}{9})$ puis $z=\frac12(\exp(\frac{i\pi}{9})+\exp(-\frac{i\pi}{9}))$ et ses puissances sont dans le sous-$\mathbb{Q}$-espace vectoriel A de $\mathbb{C}$ engendré par les nombres $x_k=\exp(\frac{ik\pi}{9})$, $0\le k\le 8$ dont un modèle est $\mathbb{Q}[X]/(X^9+1)$.
La matrice des coordonnées des z^j, $0\le j\le 9$, relativement à la famille génératrice (x_k) est de rang au plus 9 ; une relation non triviale à coefficients dans $\mathbb{Q}$ entre ses colonnes donne les coefficients d'un polynôme non nul de $\mathbb{Q}[X]$ annulant z.

⌨ Construire un tel polynôme. Est il irréductible dans $\mathbb{Q}[X]$? Voir pour ce point la partie II sur la factorisation, mais dans un premier temps on peut adapter l'instruction de niveau 3 `X=QQ['X'].gen();print(factor(1+X+X^2+X^3))`
Si le polynôme annulateur obtenu n'est pas irréductible, comment décider quel facteur irréductible annule z ?

❀ Avec Sagemath

On peut déclarer une variable X comme générateur de l'anneau de polynômes $\mathbb{Q}[X]$ par l'instruction `X=QQ['X'].gen()`.
Observer le résultat de `Q=X^9+1;print(Q.parent())`.
L'instruction `mod(k,n)` pour les entiers n'existe pas telle quelle pour les polynômes. A la place on peut déclarer une variable x comme la classe de X modulo Q par l'instruction `x=QQ['X'].quotient(Q).gen()` (pourvu que Q ait préalablement été défini).
Pour P une expression polynomiale en X, `P(x)` donne alors la classe de P dans $\mathbb{Q}[X]/Q$; `P(x).list()` donne la liste des coordonnées de la classe de P relativement à la base canonique $(1,\bar X,\dots,\bar X^{\deg(Q)-1})$; `QQ['X'](l)` donne le représentant dans $\mathbb{Q}[X]$ de degré $\le\deg(Q)-1$ de l'élément de $\mathbb{Q}[X]/(Q)$ de liste de coordonnées l relativement à la base canonique.

Reste à assembler une liste `ll` de listes de coordonnées en une matrice : `M=column_matrix(QQ,ll)` ou bien `M=matrix(QQ,ll).transpose()`.

L'instruction `M.smith_form()` donne la forme de Smith de M avec les matrices de passage, dont on peut extraire une base du noyau de M ou une relation particulière non triviale entre les colonnes de M.
L'instruction `M.charpoly()` donne le polynôme caractéristique de M. De façon moins magique on peut former la matrice $M-X\mathrm{I}$, calculer sa forme de Smith dans $\mathrm{M}_n(\mathbb{k}[X])$ pour en extraire son déterminant : `X=QQ['X'].gen();MM=M-X*identity_matrix(M.nrows());show(MM.smith_form()[0].diagonal())`.

I.B. Polynôme annulateur de $\sqrt2+\sqrt3$

On observe que le nombre $z=\sqrt2+\sqrt3$ et ses puissances entières sont dans le sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{C}$ (ou de $\mathbb{R}$) engendré par $1,\sqrt2,\sqrt3,\sqrt6$. Une relation non triviale à coefficients dans $\mathbb{Q}$ entre $1,z,z^2,z^3,z^4$ donne un polynôme annulateur de z.
On peut écrire à la main la matrice des coordonnées des z^k relativement à la famille génératrice $1,\sqrt2,\sqrt3,\sqrt6$. On peut

alternativement construire un modèle algébrique de $\mathbb{Q}[\sqrt{2},\sqrt{3}]$: $\mathbb{Q}[X,Y]/(X^2-2,Y^2-3)$ et calculer les coordonnées des puissances de $X+Y \bmod X^2-2,Y^2-3$ relativement à la base $(1,\bar{X},\bar{Y},\bar{X}\bar{Y})$.

❀ Méthodes avec Sagemath

On commence par programmer l'équivalent de l'instruction `P.list()` pour les polynômes en X,Y modulo X^2-2,Y^2-3 :

```
X,Y=QQ['X,Y'].gens()
def coef(P):
    Pmod=P%(X^2-2)%(Y^2-3)
    return([Pmod.constant_coefficient()]+[Pmod.monomial_coefficient(i) for i in [X,Y,X*Y]])
print(coef((X+Y)^2))
```

`coef(P)` rend les coordonnées du représentant canonique de $P \bmod X^2-2,Y^2-3$ relativement à la base $1,X,Y,XY$. On forme ensuite la matrice des coordonnées de $1, X+Y \bmod X^2-2,Y^2-3, \ldots, (X+Y)^4 \bmod X^2-2,Y^2-3$ et on détermine une relation non triviale entre les colonnes.

Quel polynôme annulateur de $\sqrt{2}+\sqrt{3}$ obtenez vous ? Pouvez vous en déterminer toutes les racines ?

II. L'algorithme de Kronecker de factorisation des polynômes à coefficients entiers

La factorisation d'un polynôme dans $\mathbb{Q}[X]$ se ramène à la factorisation dans $\mathbb{Z}[X]$; pourquoi ?

Soit $P \in \mathbb{Z}[X]$. On observe que si Q est un facteur de P dans $\mathbb{Z}[X]$ alors $Q(n)$ est un facteur de $P(n)$ dans $\mathbb{Z}$ pour tout entier n.
Par ailleurs si Q est de degré d, alors Q est déterminé de façon biunivoque et effective par la famille $(Q(a_0),\ldots,Q(a_d))$ dès que $a_0,\ldots,a_d$ sont des entiers distincts.
Il suffit donc, pour chaque $d \leq \frac{n}{2}$, de choisir $d+1$ entiers distincts $a_0,\ldots,a_d$ et de tester la divisibilité de P par les candidats Q déterminés par interpolation par les familles en nombre fini $(q_0,\ldots,q_d)$ où $\forall i,\ q_i \mid P(a_i)$. Attention, on ne peut pas imposer que les q_i soient tous positifs, mais on peut imposer que l'un des q_i non nul soit positif, quite à changer Q en $-Q$.

Exemple : On cherche les polynômes Q de degré 1 divisant $P=X^2+X-2$.
On choisit arbitrairement $(a_0,a_1)=(-1,0)$. On doit avoir $Q(-1) \mid P(-1)=-2$ et $Q(0) \mid P(0)=-2$ donc $Q(-1)=\pm 1,\pm 2$ tout comme $Q(0)$ ce qui fait 16 possibilités. On peut imposer $Q(-1)>0$ se qui réduit à 8 possibilités qu'on explore et on ne retient pas les éventuels polynômes constants solution :

```
X=QQ['X'].gen();P=X^2+X-2
l=[]
for a in [1,2]:
    for b in [-1,1,-2,2]:
        Q=-a*X+b*(X+1)
        if P%Q==0 and Q.degree()>=1:l+=[Q]
print(l)
```

On a avantage à choisir des entiers a_i tels que le nombre de diviseurs entiers de $P(a_i)$ soit petit. Combien y a t-il de polynômes de degré d à tester si on trouve $a_0,\ldots,a_d$ tels que $P(a_i)$ est un nombre premier pour tout i ?
Si aucun des candidats Q ne divise P cela prouve l'irréductibilité de P, d'une façon très couteuse.

❀ Méthodes avec Sagemath

On peut construire récursivement la liste des familles (q_i) d'entiers (positifs ou négatifs) divisant une famille donnée (p_i) d'entiers : `[q+l for q in diviseur([p[0]]) for l in diviseur(p[1:])]`.

Quelle taille aura cette liste en fonction de (p_i) ? On peut se restreindre à $q_0>0$ ce qui divise par deux la taille des données.

On peut construire récursivement un polynôme d'interpolation P prenant les valeurs p_i en les a_i : $P=p_0+(X-a_0)P_1$ où P_1 est un polynôme d'interpolation prenant les valeurs adéquates en les $a_i, i>0$.

Ex. Chercher de la sorte les facteurs de degré 1 puis 2 du polynôme $1-3X+X^2+X^4-3X^5+X^6$ dans $\mathbb{Z}[X]$.

Ex. Chercher les facteurs irréductibles des polynômes obtenus en I.

Int3 - 25 avr 24

Durée : 1 heure. Documents et appareils électroniques interdits. Justifiez raisonnablement chaque réponse.

Ex.1. *Rédaction.* Soit (G,·,e) un groupe noté multiplicativement, de neutre noté e, et soit $g \in G$. On suppose que le sous-groupe de G engendré par g, qu'on note $<g>$, est fini.
a. Montrer que l'ensemble des entiers $k > 0$ tels que $g^k = e$ est non vide et que son plus petit élément, disons m, est le cardinal de $<g>$.
b. Comment s'exprime l'énoncé (a) lorsque le groupe G est un groupe abélien noté additivement $(A, +, 0)$?
c. ★ Que vaut m lorsque G est le groupe additif formé des homomorphismes du groupe $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, +)$ dans lui-même et g est l'identité ?

Ex.2. Quel est le cardinal du sous-groupe de $(\mathbb{Z}/55\mathbb{Z}, +)$ engendré par x pour $x = 5$? Pour $x = 6$? Pour $x = 20$? Justifiez.

Ex.3. Le polynôme $3X^3 - 2X + 2$ est il irréductible dans $\mathbb{F}_3[X]$? dans $\mathbb{F}_5[X]$? dans $\mathbb{Z}[X]$? Justifiez convenablement.

Ex.4. On note A l'anneau $(\mathbb{Z}/55\mathbb{Z}, +, \times)$.
a. Quels sont les $a \in A$ vérifiant $a^9 = 1$?
L'application $A \to A$, $x \mapsto x^9$ est elle bijective ? (Attention aux justifications !)
b. Quels sont les $a \in A$ vérifiant $a^{10} = 1$?
★ Qu'en déduit on sur l'image de l'application $A \to A$, $x \mapsto x^{10}$?

L3 Algèbre effective - examen - 28 mai 2024

Durée 3h - Tout document et matériel électronique interdit.

Justifiez chaque réponse.

Ex.1. Répondre aux questions suivantes en détaillant raisonnablement.

1+0,5 • Quelles sont les racines de $X^2 - 1$ dans $\mathbb{Z}/12\mathbb{Z}$? Combien y en aurait il si le groupe multiplicatif $(\mathbb{Z}/12\mathbb{Z})^\times$ était cyclique ?

1 • Montrer que tout entier n est congru modulo 3 à la somme des chiffres de l'écriture décimale de n.

1 • Calculer le reste de la division euclidienne de $2234544^{1234567}$ par 15.

1 • Calculer 6^{144} modulo 315.

0,5+1 • Quelles sont les valeurs prises par l'application $x \mapsto x^3 - x$ sur $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \times)$? En déduire un exemple de polynôme irréductible de degré 3 dans $\mathbb{F}_5[X]$.

1+1 • Existe t-il un corps de cardinal 125 ? Et de cardinal 135 ? Si oui en construire un ; si non expliquer pourquoi.

Ex.2. *Calculs comme réécritures* - On part des opérations et relations primitives sur les entiers naturels (les entiers positifs ou nuls) suivantes : S (successeur), P (prédécesseur, défini sauf en 0), $=$ (égalité) et sa négation $\neq$. Ainsi, en adoptant la représentation décimale habituelle des entiers on a par exemple $S9 = 10$, $P9 = 8$, $9 \neq 10$.

On considère l'opération $*$ définie sur les entiers naturels par le système de réécritures suivant :

$$\begin{array}{lcll} (a,b) & \to & (0,0,a,b) & \\ (a,b,c,d) & \to & (Sa,Pb,c,d) & \text{si } b \neq 0 \\ & \to & (a,c,c,Pd) & \text{si } b = 0 \text{ et } d \neq 0 \\ & \to & a & \text{si } b = d = 0 \end{array}$$

1 **a.** Calculer $2 * 2$ en explicitant la suite des réécritures de $(2,2)$.

1 **b.** Montrer que la réécriture d'un quadruplet (a,b,c,d) est récursive relativement à une relation bien fondée adéquate.

1,5 Montrer par récurrence que la suite de réécritures appliquée à un quadruplet (a,b,c,d) aboutit à l'entier $a + b + cd$ (où $a + b + cd$ est interprété comme une expression usuelle dans $(\mathbb{N}, +, \cdot)$). En déduire l'expression de $a * b$ en terme des opérations
0,5 algébriques usuelles.

1,5 **c.** Par quel système de réécritures n'utilisant que les seules opérations et relations $S, P, =, \neq$ pourrait on calculer l'exponentiation habituelle a^b ? Justifier.

Ex.3. Soit (x_n) une suite à valeurs dans un ensemble S. On lui associe l'ensemble $\mathcal{P}$ formé des entiers $p \in \mathbb{Z}$ tels que $\exists n_0 \in \mathbb{N},\ \forall n \geq n_0,\ x_{n+|p|} = x_n$ (où $|p|$ désigne la valeur absolue de p). On dit que la suite (x_n) est périodique à partir d'un certain rang si l'ensemble $\mathcal{P}$ n'est pas réduit à $\{0\}$.

2 **a.** Montrer (soigneusement !) que $\mathcal{P}$ est un sous-groupe de $\mathbb{Z}$.

1 **b.** On suppose que S est fini et que (x_n) est définie par x_0 et la relation de récurrence $\forall n,\ x_{n+1} = f(x_n)$ pour $f : S \to S$ une application. Montrer que (x_n) est périodique à partir d'un certain rang.

1,5 **c.** Donner un exemple de suite (x_n) à valeur dans $\{0,1\}$ qui n'est pas périodique à partir d'un certain rang. Justifiez !

1 Donner un exemple de suite (x_n) à valeurs dans $\{0,1\}$, périodique à partir du rang 0 mais qui ne satisfait pas de relation de récurrence $x_{n+1} = f(x_n)$.

1 **d.** Exemple : Soit (x_n) la suite à valeurs dans $\mathbb{Z}/9\mathbb{Z}$ définie par $x_0 = 1\ [9]$ et $x_{n+1} = x_n + 4\ [9]$. Déterminer $\mathcal{P}$ comme sous-groupe de $\mathbb{Z}$.

1 **e.** Exemple : Soit (x_n) la suite à valeurs dans $\mathbb{Z}/7\mathbb{Z}$ définie par $\forall n,\ x_n = 2^n + 1\ [7]$. Déterminer $\mathcal{P}$.

0,5 La suite (x_n) vérifie t'elle une relation de récurrence $x_{n+1} = f(x_n)$?

f. Exemple : Soit (x_n) la suite à valeurs dans $\mathbb{Z}/7\mathbb{Z}$ définie par $x_0 = 1\ [7]$ et $x_{n+1} = 3x_n + 1\ [7]$.

1+1 Déterminer $a \in \mathbb{Z}/7\mathbb{Z}$ tel que la suite $(x_n - a)$ soit géométrique de raison $3\ [7]$. En déduire $\mathcal{P}$.

0,5 Quel serait $\mathcal{P}$ si on prenait $x_0 = 3\ [7]$?

1,5+ **g.** On considère la suite $(\bar{7}^n)_n$ dans l'anneau $\mathbb{Z}/105\mathbb{Z}$. A partir de quel rang devient elle périodique ? Quel est alors sa période ?
★ Qu'en est il dans l'anneau $\mathbb{Z}/(105^5)\mathbb{Z}$?

Ex.4. *Algèbre linéaire* - Soit la matrice $A = \begin{pmatrix} 2 & 6 & 4 \\ 4 & 6 & 8 \end{pmatrix}$. On désigne par $\mathrm{Im}(A)$ le sous-groupe de $\mathbb{Z}^2$ formé des vecteurs AX, X décrivant $\mathbb{Z}^3$.

1 **a.** Donner la liste des opérations sur les lignes et les colonnes transformant A en sa forme de Smith sur $\mathbb{Z}$.

1 En déduire les matrices inversibles (dans $\mathrm{M}_n(\mathbb{Z})$) P, Q telles que PAQ soit la forme de Smith de A.

1,5 **b.** En déduire un système d'équations modulaires de $\mathrm{Im}(A)$ vu comme sous-groupe de $\mathbb{Z}^2$.

0,5 L'application $\mathbb{Z}^3 \to \mathbb{Z}^2$ de matrice A est elle surjective ?

0,5 Qu'en est il de l'application $\mathbb{Q}^3 \to \mathbb{Q}^2$ de matrice A ?

c. Soit la matrice $B = \begin{pmatrix} 3 & 6 & 6 \\ 3 & 2 & 4 \end{pmatrix}$.

1 Pouvez vous donner un élément de $\mathrm{Im}(B)$ qui ne soit pas dans $\mathrm{Im}(A)$?

1+2 **d.** Expliciter une stratégie précise pour déterminer une base du $\mathbb{Z}$-module $\mathrm{Im}(A) \cap \mathrm{Im}(B) \subset \mathbb{Z}^2$ puis mettre en oeuvre cette stratégie.

Corr L3 alg eff. examen mai 2024

Ex 1 • On peut dresser la table

x	0	1	2	3	4	5	6	7	8	9	10	11
x^2	0	1	4	9	4	1	0	1	4	9	4	1

(dans $\mathbb{Z}/12\mathbb{Z}$, $-6 = -4 = -3 = -2 = -1$ selon les colonnes)

On observe 4 racines : $\pm 1, \pm 5$

On bien lemme des restes chinois : $\mathbb{Z}/12 \longrightarrow \mathbb{Z}/4 \times \mathbb{Z}/3$ isomorphisme d'anneaux car $4 \times 3 = 1$

$$x \longmapsto (x\,[4], x\,[3])$$

$x^2 = 1$ dans $\mathbb{Z}/12\mathbb{Z}$ $\Leftrightarrow$ $x^2 = 1$ dans $\mathbb{Z}/4\mathbb{Z}$ et $x^2 = 1$ dans $\mathbb{Z}/3\mathbb{Z}$

$x^2 - 1 = (x+1)(x-1)$. $\mathbb{Z}/3\mathbb{Z}$ est un corps donc ce produit est nul ssi $x+1 = 0$ ou $x-1 = 0$ ie $x = \pm 1$

$x^2 = 1$ dans $\mathbb{Z}/4\mathbb{Z}$ $\Rightarrow x \in (\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, -\bar{1}\}$ ces deux el^{ts} sont solutions

Donc $x^2 = 1$ dans $\mathbb{Z}/4 \times \mathbb{Z}/3$ ssi $x = (\pm 1, \pm 1)$. On reconstitue dans $\mathbb{Z}/12\mathbb{Z}$:

$(1,1) \hookleftarrow 1$

$(-1,-1) \hookleftarrow -1 = 11$

$(-1,1) \hookleftarrow 1 + 3z = -1\ [4]$

$z = 2\ [4] \rightsquigarrow 7\ [12]$

$(1,-1) = -(-1,1) \hookleftarrow -7 = 5$

• $n = \sum_{k=0}^{K} a_k 10^k$ avec $a_k \in \{0, -, 9\}$ $\rightsquigarrow$ $n\,[3] = \sum_{k=0}^{K} (a_k\,[3]) \underbrace{(10\,[3])^k}_{=1} = \sum_{k=0}^{K} (a_k\,[3]) = \left(\sum_{k=0}^{N} a_k\right)[3]$

$= 1$

• On calcul modulo 3 et modulo 5 puis on reconstitue modulo 15

$2234544\,[3] = \underbrace{2}_{1} + \underbrace{2}_{0} + \underbrace{3}_{1} + \underbrace{4}_{-1} + \underbrace{5}_{1} + \underbrace{4}_{1} + \underbrace{4}_{1}\,[3] = 0\,[3]$ donc ses puissances strictement positives aussi

$2234544\,[5] = \underbrace{2234540}_{2234540 \times 10\,[5] = 0}\,[5] + \underbrace{4\,[5]}_{=-1}$ donc $2234544^{1234567}\,[5] = (-1)^{1234567} = -1\,[5]$

1234567 est impair

On cherche donc $x\,[15]$ vérifiant $x = 0\,[3]$ et $x = -1\,[5]$

$x = -1 + 5k\ [15]$, $k = 0, 1, 2$

$x = -1 + 5 \times 2 = 9\ [15]$ convient et c'est le seul par le lemme des restes chinois.

• $315 = 5 \times 63 = 5 \times 7 \times 9$. On calcule 6^{144} modulo $5, 7, 9$ et on reconstitue modulo 315

$6^{144} = 1^{144}\,[5] = 1\,[5]$

$= (-1)^{144}\,[7] = 1^{72}\,[7] = 1\,[7]$

$= 36 \times 6^{142}\,[9] = 0\,[9]$

On cherche donc $k \in \{0, -, 34\}$ tq $9k = 1\ [5 \times 7]$

$k = 4$ convient $\rightsquigarrow$ $6^{144} = 36\ [315]$

•

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3} = -\bar{2}$	$-\bar{1}$
x^3	$\bar{0}$	$\bar{1}$	$\bar{3}$	$-\bar{3}$	$-\bar{1}$
$x^3 - x$	$\bar{0}$	$\bar{0}$	$\bar{1}$	$-\bar{1}$	$\bar{0}$

donc $x^3 - x + 2$ prend les valeurs $2, 2+1, 2-1$ dans $\mathbb{F}_5$ donc ne s'annule pas donc est irréductible puisqu'il est de degré 3

• $125 = 5^3$ $\mathbb{F}_5[X]/(X^3 - X + 2)$ est de cardinal 5^3 car est un $\mathbb{F}_5$-ev de dim 3, et est un corps car $X^3 - X + 2$ est irréductible dans $\mathbb{F}_5[X]$.

$135 = 5 \times 27$. Dans un anneau de cardinal 135 on a $135 \cdot \bar{1} = 0$ (l'ordre de 1 pour + divise 135)

Si cet anneau est un corps alors $5 \cdot \bar{1} = 0 = 27 \cdot \bar{1}$ puisque $(5 \cdot \bar{1}) \times (27 \cdot \bar{1}) = 0$

Soit $5u + 27v = 1$ une relation de Bezout entre 5 et 27 dans $\mathbb{Z}$. On a $(5u + 27v) \cdot \bar{1} = 0 + 0 = 0$ d'une part
$= \bar{1} \cdot \bar{1} = \bar{1}$ d'autre part

donc $\bar{1} = 0$ mais alors pour quelque soit x de l'anneau $x \cdot \bar{1} = 0$ et l'anneau ne peut être de cardinal 135
$= x$

Ex2 a. $(2,2) \to (0,0,2,2) \to (0,2,2,1) \to (1,1,2,1) \to (2,0,2,1) \to (2,2,2,0)$

$\downarrow$

$4 \leftarrow (4,0,2,0) \leftarrow (3,1,2,0)$

donc $2 * 2 = 4$

b. La réécriture de (a,b,c,d) est récursive relativement à l'ordre lexicographique sur (d,b) dont les éléments minimaux sont les $(a,0,c,0)$ avec $a, c \in \mathbb{N}$. Un tel élément se réécrit en $a = a + 0 + c \cdot 0$ donc l'assertion $(a,b,c,d) \dashrightarrow a + b + cd$ est vraie pour les éléments minimaux. Supposons la vraie pour tous les (a,b',c,d') avec $(d',b') < (d,b) \neq (0,0)$

si $b \neq 0$ on a $(a,b,c,d) \to (Sa, Pb, c, d)$. Par hypothèse de récurrence $(Sa, Pb, c, d) \dashrightarrow$
$Sa + Pb + cd = (a+1) + (b-1) + cd = a + b + cd$ donc l'assertion est vraie pour (a,b,c,d)

si $b = 0$ alors $d \neq 0$ (puisque on suppose $(d,b) \neq (0,0)$ ie (a,b,c,d) non minimal) alors

$(a,b,c,d) \to (a,c,c,Pd) \dashrightarrow a + c + c \cdot Pd = a + c + c(d-1) = a + c + cd - c = a + cd = a + b + cd$

par hypothèse de récurrence

donc l'assertion est vraie pour (a,b,c,d)

Conclusion : $\forall a,b,c,d \in \mathbb{N}$, $(a,b,c,d) \dashrightarrow a + b + cd$. En particulier $(0,0,a,b) \dashrightarrow ab$

donc $a * b = ab$

c. Avec l'opération $*$: $(a,b) \to (1,a,b)$

$(a,b,c) \to (a * b, b, Pc)$ si $c \neq 0$

$\to a$ si $c = 0$

Sans l'opération $*, \circ$ en reprenant sa définition : $(a,b) \to (1, 0, a, 0, b)$

$(a,b,c,d,e) \to (Sa, Pb, c, d, e)$ si $b \neq 0$

$\to (a, c, c, Pd, e)$ si $b = 0$ et $d \neq 0$

$\to (0, 0, c, a, Pe)$ si $b = 0 = d$ et $e \neq 0$

$\to a$ si $b = d = e = 0$

La réécriture de (a,b,c,d,e) est récursive relativement à l'ordre lexicographique sur (e,d,b). On montre par récurrence relativ à cet ordre qu'elle aboutit à $(a + b + d \cdot c)^e \cdot c^e$, en particulier à a^b si on part de $(1,0,a,0,b)$.

Ex 3. a. $\mathcal{P} = \{ p \in \mathbb{Z},\ \exists n_0 \in \mathbb{N},\ \forall n \geq n_0,\ x_{n+|p|} = x_n \}$. On veut montrer que $\mathcal{P}$ est un ss-groupe de $\mathbb{Z}$, donc que (1) $0 \in \mathcal{P}$; (2) $\forall p \in \mathcal{P}, -p \in \mathcal{P}$; (3) $\forall p, p' \in \mathcal{P},\ p+p' \in \mathcal{P}$

(1) et (2) sont vrais d'après l'expression de $\mathcal{P}$. Montrons (3)

On a $p+p' \in \mathcal{P} \iff -(p+p') \in \mathcal{P}$. Quitte à changer p, p' en leurs opposés on peut se ramener à $p+p' \geq 0$

Quitte à échanger p avec p', on peut alors supposer $p \geq 0$.

Soit n_0 tq $\forall n \geq n_0,\ x_{n+p} = x_n$

n_1 —— n_1 $x_{n+|p'|} = x_n$

Si $p' \geq 0$ on a $x_{n+p+p'} = x_{n+p}$ dès que $n+p \geq n_1$ donc dès si $n \geq n_1$ (condition suffisante)

$= x_n$ si de plus $n \geq n_0$ donc si $n \geq \max(n_0, n_1)$ d'où $p+p' \in \mathcal{P}$

Si $p' < 0$ on a $x_{n+p+p'} = x_{\underbrace{(n+p+p')}_{n+p} + |p'|}$ dès que $\underbrace{n+p+p'}_{\geq 0} \geq n_1$ donc si $n \geq n_1$ (cond. suff.)

$= x_n$ si de plus $n \geq n_0$ donc si $n \geq \max(n_0, n_1)$ d'où $p+p' \in \mathcal{P}$

Dans tous les cas $p+p' \in \mathcal{P}$, CQFD

b. $f : S \to S$ avec S fini, $x_0 \in S$, $\forall n, x_{n+1} = f(x_n)$

$\begin{cases} \mathbb{N} \to S \\ n \mapsto x_n \end{cases}$ ne peut pas être injective puisque $\mathbb{N}$ est infini et S fini, donc il existe $i < j$ tq $x_i = x_j$

On montre par récurrence sur $n \in \mathbb{N}$ que l'on a $x_{n+i} = x_{n+j}$: c'est vrai pour $n = 0$ et si c'est vrai pour n alors $\underbrace{f(x_{n+i})}_{x_{n+1+i}} = \underbrace{f(x_{n+j})}_{x_{n+1+j}}$

Dit autrement on a $\forall n \geq 0\ \ x_{n+i} = x_{n+i+(j-i)}$ donc $\forall n \geq i\ \ x_n = x_{n+(j-i)}$ donc $\underbrace{j-i}_{\neq 0} \in \mathcal{P}$

c. 1) Posons $x_n = 1$ si $n = 2^k$ pour un $k \in \mathbb{N}$

$= 0$ sinon

Supposons (x_n) périodique de période p à partir d'un rang n_0. Choisissons k tq $2^k > \max(n_0, p)$

alors $x_{2^k+1} = x_{2^k+2} = \dots = x_{2^k+p} = 0$ puisque $2^k + p < 2^k + 2^k = 2^{k+1}$, et par périodicité $x_{2^k+2^k} = x_{2^k + 2^k \% p}$

$= 0$

en contradiction avec $x_{2^{k+1}} = 1$

2) Posons $x_n = 0$ si $n = 0$ ou 1 [3] alors $\forall n, x_n = x_{n\%3} = x_{n+3}$ donc : (x_n) est périodique

$= 1$ si $n = 2$ [3]

de période 3. S'il existait $f : \{0,1\} \to \{0,1\}$ tq $\forall n, x_{n+1} = f(x_n)$ on aurait $f(0) = x_1 = 0$

mais alors $x_2 = f(x_1) = f(0) = 0$ en contradiction avec $x_2 = 1$

(Ex3) d. $x_0 = 1\ [9]$, $x_{n+1} = x_n + 4\ [9]$ alors $\forall n, x_n = 1 + 4n\ [9]$

On a $x_{n+p} = x_n \Leftrightarrow 1 + 4(n+p) = 1 + 4n\ [9] \Leftrightarrow 4p = 0\ [9] \Leftrightarrow p = 0\ [9]$ car $4 \wedge 9 = 1$

donc $\mathcal{P} = 9\mathbb{Z}$

e. $x_n = 2^n + 1\ [7]$ On a $x_{n+p} = x_n \Leftrightarrow 2^{n+p} + 1 = 2^n + 1\ [7]$

$\Leftrightarrow 2^n 2^p = 2^n\ [7]$

$\Leftrightarrow 2^p = 1\ [7]$ car $\forall n\ 2^n \in \mathbb{U}_{7\mathbb{Z}}^{\times}$

$\Leftrightarrow p$ est un multiple de l'ordre de 2 dans $\mathbb{U}_{7\mathbb{Z}}^{\times}$

On a $2^1, 2^2 \neq 1$ ds $\mathbb{U}_{7\mathbb{Z}}$ et $2^3 = 1$ ds $\mathbb{U}_{7\mathbb{Z}}$ donc l'ordre de 2 ds $\mathbb{U}_{7\mathbb{Z}}^{\times}$ est 3 ; donc $\mathcal{P} = 3\mathbb{Z}$.

On observe $x_{n+1} = 2^{n+1} + 1\ [7] = 2(2^n + 1) - 1 = 2x_n - 1\ [7]$ donc $x_{n+1} = f(x_n)$ avec

$f : \mathbb{U}_{7\mathbb{Z}} \to \mathbb{U}_{7\mathbb{Z}}$, $x \mapsto 2x - 1$

f. 1) $x_0 = 1\ [7]$ et $\forall n\ x_{n+1} = 3x_n + 1\ [7]$

On a $\underbrace{x_{n+1} - a}_{3x_n + 1 - a} = 3(x_n - a) \Leftrightarrow 1 - a = -3a\ [7] \Leftrightarrow +2a = -1\ [7]$

$\Leftrightarrow a = \underbrace{-4\ [7]}_{3\ [7]}$ car 2 est inversible d'inverse 4 ds $\mathbb{U}_{7\mathbb{Z}}$

On obtient $\forall n\ x_n - 3 = (x_0 - 3) \cdot 3^n\ [7] = 5 \cdot 3^n\ [7]$

On a $x_{n+p} = x_n \Leftrightarrow \underbrace{x_{n+p} - 3}_{5 \cdot 3^{n+p}\ [7]} = \underbrace{x_n - 3}_{5 \cdot 3^n\ [7]} \Leftrightarrow 3^p = 1\ [7]$ car $5 \cdot 3^n \wedge 7 = 1$

$\Leftrightarrow p$ est un multiple de l'ordre de 3 ds $\mathbb{U}_{7\mathbb{Z}}^{\times}$

$3^1, 3^2, 3^3 \neq 1\ [7]$ et l'ordre de 3 divise $|\mathbb{U}_{7\mathbb{Z}}^{\times}| = 6$ donc l'ordre de 3 ds $\mathbb{U}_{7\mathbb{Z}}^{\times}$ est 6.

Conclusion $\mathcal{P} = 6\mathbb{Z}$.

2) $x_0 = 3$, $x_{n+1} = 3x_n + 1\ [7]$ alors $x_1 = 10\ [7] = 3\ [7] = x_0$ puis par récurrence $\forall n, x_n = x_0$

de sorte que $\mathcal{P} = \mathbb{Z}$

g. $x_n = 7^n$ dans $\mathbb{U}_{105\mathbb{Z}}$. On a $105 = 5 \times 21 = 5 \times 3 \times 7$.

$7^{n+p} = 7^n\ [105] \Leftrightarrow 7^{n+p} = 7^n$ modulo 3, 5 et 7 par le théorème des restes chinois.

On a $7 = 1\ [3]$ donc $7^{n+p} = 7^n\ [3]$ quelque soit $p \in \mathbb{N}$

$7 = 2\ [5]$; $7^{n+p} = 7^n\ [5] \Leftrightarrow 2^n 2^p = 2^n\ [5] \Leftrightarrow 2^p = 1\ [5]$ car $2^n \wedge 5 = 1$

$\Leftrightarrow 4 \mid p$ car 2 est d'ordre 4 ds $\mathbb{U}_{5\mathbb{Z}}^{\times}$

$7^n = 0\ [7]$ dès que $n \geq 1$ donc $7^{n+p} = 7^n\ [7] \Leftrightarrow n \geq 1$ et p quelconque

Conclusion $7^{n+p} = 7^n\ [105] \Leftrightarrow n \geq 1$ et $4 \mid p$: (7^n) est périodique de période 4 ds $\mathbb{U}_{105\mathbb{Z}}$ à partir du rang 1

(Ex3 g)

$\mathbb{Z}/10^5\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/3^5\mathbb{Z} \times \mathbb{Z}/5^5\mathbb{Z} \times \mathbb{Z}/7^5\mathbb{Z}$ comme anneau

$x \longmapsto (x[3], x[5], x[7])$

$(7^n)_n$ est périodique dès $n=0$ de période l'ordre de 7 ds $(\mathbb{Z}/3^5\mathbb{Z})^\times$ comme dans $(\mathbb{Z}/5^5\mathbb{Z})^\times$

$7^n = 0$ dès que $n \geq 5$ ds $\mathbb{Z}/7^5\mathbb{Z}$

Donc dans $\mathbb{Z}/10^5\mathbb{Z}$ (7^n) est périodique de période ppcm (ordre $(7, (\mathbb{Z}/3^5\mathbb{Z})^\times)$, ordre $(7, (\mathbb{Z}/5^5\mathbb{Z})^\times)$) à partir du rang $n=5$

Ordre $(7, (\mathbb{Z}/3^5\mathbb{Z})^\times)$ est un diviseur de $\varphi(3^5) = 2\times 3^4$. Pour les déterminer précisément mieux vaut

— $(7, (\mathbb{Z}/5^5\mathbb{Z})^\times)$ — $\varphi(5^5) = 4\times 5^4$

connaître d'avance la question : $7 = 1+2\times 3 \in \ker\left((\mathbb{Z}/3^5\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times, x \mapsto x[3]\right) \simeq (\mathbb{Z}/3^4\mathbb{Z}, +)$ est un générateur

$7 = 2\,[5]$ est d'ordre 4 dans $(\mathbb{Z}/5\mathbb{Z})^\times \rightsquigarrow 7^4 \in \ker\left((\mathbb{Z}/5^5\mathbb{Z})^\times \to (\mathbb{Z}/5\mathbb{Z})^\times\right)$

On observe $7^2 = -1+2\times 5^2 \rightsquigarrow 7^4 = 1 - 4\times 5^2 + 5^4 = 1 + 5^2\,[5^3]$

et on sait (?) $1+5^2$ est d'ordre 5^3 dans $\ker\left((\mathbb{Z}/5^5\mathbb{Z})^\times \to (\mathbb{Z}/5\mathbb{Z})^\times\right) \simeq (\mathbb{Z}/5^4\mathbb{Z}, +)$

On en déduit que 7 est d'ordre 4×5^3 dans $(\mathbb{Z}/5^5\mathbb{Z})^\times$

Finalement 7 est d'ordre $\text{ppcm}(2\times 3^4, 4\times 5^3) = 4\times 3^4\times 5^3$ dans $\mathbb{Z}/10^5\mathbb{Z}$

< Vérification avec Sagemath : `mod(7, 15^5).multiplicative_order()` ok ! >

Ex4. cf corrigé Session 2 - juin 22 ex 5 ou de exam mai 21 ex 3

a. $A = \begin{pmatrix} 2 & 6 & 4 \\ 4 & 6 & 8 \end{pmatrix} = 2\begin{pmatrix} 1 & 3 & 2 \\ 2 & 3 & 4 \end{pmatrix} \xrightarrow[L_2 \to L_2 - 2L_1]{} 2\begin{pmatrix} 1 & 3 & 2 \\ 0 & -3 & 0 \end{pmatrix} \xrightarrow[\substack{C_2 \to C_2 - 3C_1 \\ C_3 \to C_3 - 2C_1}]{} 2\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix} \xrightarrow[C_2 \to -C_2]{} 2\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = D$

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow[L_2 \to L_2 - 2L_1]{} \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = P$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[\substack{C_2 \to C_2 - 3C_1 \\ C_3 \to C_3 - 2C_1}]{} \xrightarrow[C_2 \to -C_2]{} \begin{pmatrix} 1 & 3 & -2 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = Q$ $\quad PAQ = D$

b. $\text{Im}\, D \ni (x,y) \Leftrightarrow \begin{cases} x = 0\,[2] \\ y = 0\,[6] \end{cases}$. $\begin{pmatrix} x \\ y \end{pmatrix} \in \text{Im}\, A \overset{\uparrow}{\Leftrightarrow} P\begin{pmatrix} x \\ y \end{pmatrix} \in P\,\text{Im}\, A = \text{Im}\, PA \overset{\uparrow}{\Leftrightarrow} P\begin{pmatrix} x \\ y \end{pmatrix} \in \text{Im}\, PAQ$

car P inversible ; car Q inversible

$\Leftrightarrow \begin{cases} x = 0\,[2] \\ -2x + y = 0\,[6] \end{cases}$

$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \notin \text{Im}\, A$ d'après bon syst. d'équations donc $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto A\begin{pmatrix} x \\ y \\ z \end{pmatrix}$, $\mathbb{Z}^3 \to \mathbb{Z}^2$ n'est pas surjective.

Le syst. d'équations est toujours satisfait sur $\mathbb{Q}$ donc l'appl. $\mathbb{Q}^3 \to \mathbb{Q}^2$ est surjective.

c. $\begin{pmatrix} 3 \\ 3 \end{pmatrix} = B\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in \text{Im}\, B$ mais ne satisfait pas le syst. d'eq. de $\text{Im}\, A$.

(Ex 4) d. Une stratégie possible est de déterminer un système d'équations de $\mathrm{Im}\, B$ comme on l'a fait pour $\mathrm{Im}\, A$, de le concaténer avec le syst. obtenu pour $\mathrm{Im}\, A$ puis de chercher une base des solutions du système concaténé.

$$B = \begin{pmatrix} 3 & 6 & 6 \\ 3 & 2 & 4 \end{pmatrix} \xrightarrow[C_1 \to C_1 - C_2]{} \begin{pmatrix} -3 & 6 & 6 \\ 1 & 2 & 4 \end{pmatrix} \xrightarrow[\substack{C_2 \to C_2 - 2C_1 \\ C_3 \to C_3 - 4C_1}]{} \begin{pmatrix} -3 & 12 & 18 \\ 1 & 0 & 0 \end{pmatrix} \xrightarrow[L_2 \to L_1 + 3L_2]{} \begin{pmatrix} 0 & 12 & 18 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\left| C_2 \to C_2 - C_3 \right.$$

$$D_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6 & 0 \end{pmatrix} \xleftarrow[L_1 \leftrightarrow L_2]{} \begin{pmatrix} 0 & -6 & 0 \\ 1 & 0 & 0 \end{pmatrix} \xleftarrow[C_3 \to C_3 + 3C_2]{} \begin{pmatrix} 0 & -6 & 18 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow[L_1 \to L_1 + 3L_2]{} \xrightarrow[L_2 \leftrightarrow L_2]{} \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} = P \quad \cdot \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow[C_1 \to C_1 - C_2]{} \dashrightarrow Q \quad \text{mais on n'en a pas besoin.}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{Im}\, B \Leftrightarrow P\begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{Im}\, PB = \mathrm{Im}\, PBQ = \mathrm{Im}\, D_B \Leftrightarrow \begin{cases} y = 0 \ [1] \\ x + 3y = 0 \ [6] \end{cases} \Leftrightarrow x + 3y = 0 \ [6]$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{Im}\, A \cap \mathrm{Im}\, B \Leftrightarrow \begin{cases} x = 0 \ [2] & (1) \\ y - 2x = 0 \ [6] & (2) \\ x + 3y = 0 \ [6] & (3) \end{cases}$$

que on résout : $y = 2x + 6k$ pour un $k \in \mathbb{Z}$ par (2)

$x = 2x'$ par (1)

$2x' + 12x' + 18k = 0 \ [6] \Leftrightarrow x' = 0 \ [3]$

$\Leftrightarrow x' = 3\ell$ pour un $\ell \in \mathbb{Z}$

On obtient $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{Im}\, A \cap \mathrm{Im}\, B \Leftrightarrow \exists k, \ell \in \mathbb{Z},\ \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 6\ell \\ 12\ell + 6k \end{pmatrix} = k\begin{pmatrix} 0 \\ 6 \end{pmatrix} + \ell\begin{pmatrix} 6 \\ 12 \end{pmatrix}$

$\Leftrightarrow (x, y) \in \langle (0,6), (6,12) \rangle \rightsquigarrow \big((0,6), (6,12)\big)$ est une $\mathbb{Z}$-base de $\mathrm{Im}\, A \cap \mathrm{Im}\, B$

manifestement linéairement indépendants.

$R_4 \langle (0,6), (6,12) \rangle = \langle (0,6), (6,0) \rangle = 6\mathbb{Z}^2$

L3 Algèbre effective - session 2 - 2 juillet 2024

Durée 3h - Tout document et tout matériel électronique interdit.

Justifiez chaque réponse.
On pourra librement utiliser le fait que le groupe multiplicatif d'un corps fini est cyclique.

Ex.1. Répondre aux questions suivantes en détaillant raisonnablement.

1 **a.** Calculer $12825 \% 55$ (le reste de la division euclidienne par 55).

1 **b.** Calculer $12825 \wedge 55$ (le plus grand diviseur commun).

2 **c.** Calculer le reste de la division euclidienne de $2234544^{1234567}$ par 55.

2 **d.** Combien y a t-il d'éléments d'ordre exactement 2 dans le groupe multiplicatif $(\mathbb{Z}/35\mathbb{Z})^\times$?
1 Combien de racines possède le polynôme $X^2 - 1$ dans l'anneau $\mathbb{Z}/55\mathbb{Z}$?
1 Combien de racines possède le polynôme $X^2 + 1$ dans l'anneau $\mathbb{Z}/55\mathbb{Z}$?

1+1+1 **e.** Le polynôme $X^4 + X^3 + X^2 + X + 1$ est il irréductible dans $\mathbb{F}_2[X]$? dans $\mathbb{F}_5[X]$? dans $\mathbb{Z}[X]$?

Ex.2 *Objet bien défini, algorithme de calcul*

1,5 **a.** Qu'est ce qu'une relation de Bezout pour un triplet d'entier (a, b, c) ? Et pour un triplet de polynômes (A, B, C) de $\mathbb{Q}[X]$?

2 **b.** Ecrire un algorithme élémentaire (avec les opérations algébriques usuelles sur les entiers et la division euclidienne) de calcul d'**une** relation de Bézout pour un triplet d'entier (a, b, c).

2 **c.** Mettez en oeuvre l'algorithme détaillé en (b) sur le triplet $(6, 15, 10)$. Qu'obtenez vous ?

Ex.3. *Rédaction - On admet que tout polynôme de $\mathbb{C}[X]$ de degré ≥ 1 admet au moins une racine dans $\mathbb{C}$.*
Soient A, B deux polynômes non nuls de $\mathbb{Q}[X]$ sans racine complexe commune.

1,5 1 **a.** Montrer que A et B sont premier entre eux dans $\mathbb{Q}[X]$.

b. Montrer à l'aide d'une relation de Bézout adéquate et **sans utiliser un argument d'autorité "c'est vrai d'après tel théorème..."** qu'on a

1 $\forall P \in \mathbb{Q}[X],\ (A \text{ divise } BP \Leftrightarrow A \text{ divise } P)$.

1 En déduire que si A et B divise un même polynôme P dans $\mathbb{Q}[X]$ alors le produit AB divise P.

1 **c.** Quel est le noyau de l'application $\Phi : \mathbb{Q}[X] \to (\mathbb{Q}[X]/A) \times (\mathbb{Q}[X]/B),\ P \mapsto (P \bmod A,\ P \bmod B)$?

1 Qu'en déduit on sur la dimension de $\mathrm{Im}(\Phi)$ comme $\mathbb{Q}$-espace vectoriel ?

Ex.4. *Interpolation dans $\mathbb{Z}[X]$* - Soient $n \geq 0$ et $a_0, \ldots, a_n, b_0, \ldots, b_n$ des entiers. On s'intéresse au problème d'interpolation
(I) $\forall i \in \{0, \ldots, n\},\ P(a_i) = b_i$
d'inconnu $P \in \mathbb{Z}[X]$.

1 **a.** *Approche arithmétique* - Montrer que si $P \in \mathbb{Z}[X]$ satisfait (I) alors P s'écrit $P = b_0 + (X - a_0)P_1$ avec $P_1 \in \mathbb{Z}[X]$.

1 Quelles équations vérifient alors les valeurs prises par P_1 en $a_1, \ldots, a_n$? En déduire un algorithme récursif de calcul des P
1 solution.

1 **b.** *Exemple :* Quels sont les $P \in \mathbb{Z}[X]$ (s'ils existent) vérifiant les trois conditions $P(2) = 3$, $P(3) = 6$ et $P(4) = 13$?

c. *Approche matricielle* - Pour $d \geq 0$ on note V_d le groupe abélien (ou $\mathbb{Z}$-module) formé des polynômes de $\mathbb{Z}[X]$ de degré $\leq d$ et Φ l'application $V_d \to \mathbb{Z}^{n+1},\ P \mapsto (P(a_0), \ldots, P(a_n))$.

1 Déterminer la matrice de l'application Φ relativement à la $\mathbb{Z}$-base $(1, X, \ldots, X^d)$ de V_d et à la base canonique de $\mathbb{Z}^{n+1}$.

1 Quelle équation matricielle doit vérifier le vecteur colonne des coordonnées de P relativement à la base $(1, X, \ldots, X^d)$ pour
que P satisfasse (I)

d. Déterminer la forme de Smith de la matrice

$$A = \begin{pmatrix} 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \\ 1 & 4 & 16 & 64 \end{pmatrix}$$

En déduire un système d'équation modulaire du sous-groupe $\mathrm{Im}(A) \subset \mathbb{Z}^3$.

e. A t-on $(2, 6, 13) \in \mathrm{Im}(A)$? Qu'en déduit on sur le problème (I) ?

Quels sont les $X \in \mathbb{Z}^4$ solutions de $AX = \begin{pmatrix} 3 \\ 6 \\ 13 \end{pmatrix}$? Quelles solutions obtient on ainsi pour la question 4.b plus haut ?

Ex.5.★ Donner et mettre en oeuvre une stratégie de calcul d'un polynôme non nul de $\mathbb{Q}[X]$ annulateur de $2^{\frac{1}{3}} + 3^{\frac{1}{2}}$.