PRÉPAS ELBILIA
GROUPE ELBILIA · LÉON L'AFRICAIN

Prépas MP

My Ismail Mamouni

http ://myismail.net

مَـمُـوُنِي مُولَايِ اسمَاعِيل

Support de Cours

Algèbe Générale

Table des matières

1 Au commencement...

1.1 De brefs rappels

Théorème 1 *division euclidienne*
Pour tout couple d'entiers naturels (a, b) tel que $b > 0$, il existe un couple (q, r) et un seul vérifiant :

$$a = bq + r \text{ et } 0 \leq r < b.$$

Exercice 1

1. Décrire un algorithme de division euclidienne en n'utilisant que la soustraction comme opération arithmétique, produire par la même occasion la preuve du théorème précédent ;
2. Écrire un programme récursif qui prend a et b en données et retourne le couple (q, r); (7.1)

Définition 1 *diviseurs, nombres premiers, ppcm, pgcd*
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ deux entiers.

division euclidienne La division euclidienne est l'application

$$\phi : (a, b) \in \mathbb{N} \times \mathbb{N}^* \to (q, r) \in \mathbb{N}^2$$

où q et r, définis par le théorème précédent, ie : $0 \leq r < b$, sont respectivement le quotient et le reste dans la division euclidienne de a par b;

divisibilité
on dit que a divise b (ou que b est un multiple de a) et on note $a|b$ ssi il existe $k \in \mathbb{Z}$, $b = ka$;

nombre premier
$p \in \mathbb{Z}$ est premier ssi $p \neq 1$ et si ses seuls diviseurs sont ± 1 et $\pm p$;

nombres premiers entre eux ou étrangers
deux entiers sont premiers entre eux ssi leurs seuls diviseurs communs sont 1 et -1 ;

pgcd
on note pgcd(a,b), le plus grand diviseur commun à a et b;

ppcm
on note ppcm(a,b), le plus petit multiple positif commun à a et b;

relation de congruence modulo n
Soit n un entier non nul. La relation de congruence modulo n est la relation définie sur $\mathbb{Z}^2$ par :

$$a \equiv b[n] \Leftrightarrow a - b \in n\mathbb{Z}.$$

1.2 Algorithme d'Euclide, identité de Bezout

Exercice 2 *l'algorithme d'Euclide et sa programmation*

1. Soient a et b deux entiers, (q, r) le résultat de la division euclidienne de a par b :

$$a = bq + r,\ 0 \leq r < b.$$

   Justifier que (a, b) et (b, r) ont le même pgcd.

2. On note $r_0 = a,\ r_1 = b$, et, tant que $r_i \neq 0$, $r_{i-1} = r_i q_i + r_{i+1}$ avec $0 \leq r_{i+1} < r_i$. Montrer que la suite obtenue est finie, que son dernier terme est nul et que le dernier reste non nul est le pgcd de a et b.

3. Montrer qu'il existe des entiers u et v tels que $pgcd(a, b) = au + bv$. On pourra exprimer matriciellement $\begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix}$ en fonction de $\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$.

4. Écrire un programme MAPLE qui prend a et b en arguments et retourne un triplet (d, u, v) tel que $d = pgcd(a, b) = au + bv$. Voir en section 7.1.

Théorème 2 *algorithme d'Euclide, identité de Bezout*
• Si a et b sont deux entiers naturels non nuls, la suite définie par l'algorithme :
– $r_0 = a, r_1 = b$,
– tant que $r_{i+1} \neq 0, r_{i+2}$ est le reste dans la DE de r_i par r_{i+1},
est finie.
Cela signifie que l'algorithme termine (sic). La dernière itération donne $r_m = 0$ et le dernier reste non nul, r_{m-1} est le pgcd de a et b.
• Il existe u, v entiers relatifs tels que

$$pgcd(a, b) = au + bv;$$

(identité de Bezout)

Démonstration c'est l'exercice précédent ; on notera toutefois que l'on peut calculer pratiquement les coefficients de Bezout de la façon suivante : si r_n est le dernier reste non nul, on a $r_{n-2} - r_{n-1}q_{n-1} = r_n$, on remplace alors r_{n-1} et r_{n-2} en usant des relations $r_{i-1} - r_i q_i = r_{i+1}$.

Théorème 3 *théorème de Bezout*
Pour tout couple d'entiers naturels $(a, b) \in \mathbb{N}^2$, a et b sont premiers entre eux ssi il existe des entiers relatifs u v, tels que $1 = ua + bv$.

Démonstration
$\Rightarrow$ conséquence de l'algorithme d'Euclide étendu ;
$\Leftarrow$ on observe qu'un diviseur commun à a et b divise 1 ;

Exercice 3 *théorème de Lamé (1845) ou pourquoi MAPLE est utilisable*

On se propose ici d'évaluer le nombre d'opérations réalisées par l'algorithme d'Euclide lors d'une exécution avec comme données a et b.

1. La suite de Fibonacci (Léonard de Pise [1]) est définie de la façon suivante :

$$F_0 = 0,\ F_1 = 1 \text{ et } F_{n+2} = F_{n+1} + F_n.$$

Donner une expression de F_n en fonction de n; vérifier que deux termes successifs de la suite $(F_n)_{n\geq 1}$ sont premiers entre eux.

2. On suppose dorénavant que $a > b$. On note $r_0 = a,\ r_1 = b$, $r_{i-1} = r_i q_i + r_{i+1}$ avec $0 \leq r_{i+1} < r_i$. La suite obtenue est celle des restes dans l'algorithme d'Euclide. Montrer que si n est le nombre d'itérations de l'algorithme d'Euclide, alors

$$a \geq F_{n+1},\ b \geq F_n.$$

Indication : écrire en colonne 1 la succession des opérations de l'algorithme d'Euclide (on notera r_n le dernier reste non nul) ; écrire en colonne 2, en commençant par la dernière ligne et après les avoir justifiées, des inégalités vérifiées par les $G_i = r_{n-i+1}$.

r_0	$= q_1 r_1 + r_2$	$G_?$	$\geq G_? + G_?$
r_1	$= q_2 r_2 + r_3$		
r_3	$= q_3 r_3 + r_4$		
$\vdots$		$\vdots$	
r_{i-1}	$= q_i r_i + r_{i+1}$	$G_?$	$\geq G_? + G_?$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-2}	$= q_{n-1} r_{n-1} + r_n$	G_3	$\geq G_2 + G_1$
r_{n-1}	$= q_n r_n + r_{n+1}$	G_2	$\geq G_1 + G_0$

3. En déduire une majoration de n en fonction des données a et b.

C'est parce que son coût est en $O(\ln(\sup(a,b))$ que l'algorithme d'Euclide est efficient... Cette étude est aussi développée dans un sujet EPITA 2004.

1.3 Décomposition en facteurs premiers

Théorème 4 *théorème de Gauss*

• Si deux entiers a et b sont premiers entre eux, alors $a|\, b\, x \Rightarrow a|x$.

• si p est premier, alors $p|\, ab \Rightarrow p|a$ ou $p|b$.

Démonstration : on fera appel au théorème de Bezout pour écrire une relation $au+bv = 1$ puis $axu + bxv = x$...

1. Attention : Lamé (XIX° siècle) n'est pas disciple de Léonard (XII° siècle)

Théorème 5 *théorème fondamental de l'arithmétique*
Tout entier naturel $n > 1$ est d'une façon et d'une seule produit de facteurs premiers :

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$$

où les α_p non nuls sont en nombre fini.

Démonstration
on procède par récurrence tant en ce qui concerne l'existence que l'unicité :

Exercice 4 *niveau collège, pour mémoire*
Soient $n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$ et $m = \prod_{p \in \mathcal{P}} p^{\beta_p}$.

1. Exprimer les pgcd et ppcm de n et de m;
2. Justifier que $\nu = n/d$ et $\mu = m/d$ sont premiers entre eux lorsque $d = pgcd(n, m)$; exprimer le ppcm de n et m en fonction de ces trois nombres ;

Exercice 5
Démontrer qu'il existe une infinité de nombres premiers. Raisonner par l'absurde en posant $P = \prod p_k \cdots$

Exercice 6 *Centrale 2003*
Soit $n \in \mathbb{N}^*$, on note $S(n)$ le nombre de diviseurs de n dans $\mathbb{N}^*$.

1. Exprimer $S(n)$ à l'aide de la décomposition en nombres premiers. Commencer par $n = p^\alpha, p$ premier ;
2. On note E_p l'ensemble des n tels que $S(n) = 2p$. Montrer que si p et $2^p - 1$ sont tous deux premiers, $2^{p-1}(2^p - 1) \in E$.
3. Soit n pair, $n \in E_p$. Comment peut-on l'écrire ?

Exercice 7 *brèves*

1. Montrer que si p est un nombre premier supérieur ou égal à 5, $24 | p^2 - 1$ (Mines)
2. Partant de l'écriture de n en base 10, on enlève le dernier chiffre, qu'on retranche deux fois au nombre ainsi découpé. On obtient m, qui est divisible par 7 ssi n l'est. Formalisez et prouvez.
   Exemple : $31976 \to 3197 - 2 \times 6 = 3185 \to 318 - 2 \times 5 = 308 \to 30 - 2 \times 8 = 14$ qui est divisible par 7.

Exercice 8 *nombres premiers d'une forme particulière*

1. Soit q un entier. Factoriser dans $\mathbb{Z}[X]$ les polynômes $X^q - 1$ et $X^q + 1$;
2. Soient $a > 1$ et $n > 0$, deux entiers. Montrer que si $a^n + 1$ est premier alors n est une puissance de 2.

voir aussi l'exercice 9.

Exercice 9 *nombres de Mersenne, nombres de Fermat*
Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (nombres de Fermat).

1. Calculer les premiers termes de cette suite, conjecturer, déconjecturer.
2. Comparer le produit $\prod_{k=0}^{n} F_k$ à F_{n+1}. Conjecturer et démontrer.
3. Montrer que, si $n \neq m$, F_n et F_m sont premiers entre eux.

Exercice 10 *produits de Cauchy, produits infinis et nombres premiers*

1. Soit $p \geq 2$ un entier. Que vaut la somme
$$\sum_{s=0}^{\infty} \frac{1}{p^s} ?$$
2. Déterminer le produit de Cauchy des séries géométriques $\sum \frac{1}{2^p}$ et $\sum \frac{1}{3^p}$.
3. Donner une expression judicieuse de $\frac{1}{\left(1-\frac{1}{2}\right)} \frac{1}{\left(1-\frac{1}{3}\right)} \frac{1}{\left(1-\frac{1}{5}\right)}$ sous forme de série.
On note T_n la $n^{ième}$ somme partielle de cette série. Développer T_2 et montrer que l'on a l'encadrement
$$H(6) \leq T_2 \leq H(25)$$
dans lequel $H(n)$ désigne la somme partielle de la série harmonique $H(n) = \sum_{k=1}^{n} \frac{1}{k}$.
4. On note $(p_n)_n$ la suite des nombres premiers (ainsi $p_1 = 2, p_2 = 3, p_3 = 5, p_8 = 19$ etc...). On définit une suite $(\mathcal{P}_n)_n$ en posant
$$\mathcal{P}_n = \prod_{k=1}^{n} \frac{1}{\left(1-\frac{1}{p_k}\right)}.$$
   (a) Montrer que
   $$\mathcal{P}_n = \sum_{m=0}^{\infty} \theta_{n,m} \text{ où } \theta_{n,m} = \sum_{(\alpha_1+...+\alpha_n)=m} \frac{1}{2^{\alpha_1}} \frac{1}{3^{\alpha_2}} ... \frac{1}{p_n^{\alpha_n}}.$$
   (b) On considère la somme partielle $\mathcal{P}_n^N = \sum_{m=0}^{N} \theta_{n,m}$. Montrer que $\mathcal{P}_n^N \leq H(p_n^N)$.
   (c) Soit K un entier compris entre 1 et $\min(2^N, p_n)$. On suppose que K se décompose en $K = 2^{a_1} 3^{a_2} ... p_j^{a_j}$.
   Justifier que tout nombre premier p_i figurant dans cette décomposition avec $a_i > 0$ est inférieur à p_n et que $a_1 + a_2 + ... + a_j \leq N$.
   (d) Démontrer que pour tout $(n, N) \in \mathbb{N}^2$, il existe un entier q, que vous déterminerez, tel que $H(q) \leq \mathcal{P}_n^N$. En déduire que $H(q) \leq \mathcal{P}_n$ puis que $\lim \mathcal{P}_n = +\infty$.
5. Déterminer la nature de la série $\sum \ln\left(1-\frac{1}{p_k}\right)$.
6. Montrer que la série $\sum \frac{1}{p_k}$ diverge.

2 Congruences : l'anneau $\mathbb{Z}/n\mathbb{Z}$

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

Théorème 6 *sous-groupes de* $(\mathbb{Z}, +)$
Une partie H est un sous-groupe de $\mathbb{Z}$ ssi il existe un entier a non nul tel que $H = a\mathbb{Z}$.

Démonstration :
$\Leftarrow$: facile et immédiat
$\Rightarrow$: division euclidienne ;

Définition 2 *relation de congruence, classes de congruence*
Soit n un entier non nul. La relation de congruence modulo n est la relation définie sur $\mathbb{Z}^2$ par :

$$a \equiv b[n] \Leftrightarrow a - b \in n\mathbb{Z}.$$

Proposition 7 *classes*

1. La relation de congruence modulo n a les propriétés suivantes (qui en font une relation d'équivalence (voir rappel en annexe, pas de démonstration !)) :
   - $a \equiv a[n]$;
   - $a \equiv b[n] \Rightarrow b \equiv a[n]$;
   - $a \equiv b[n]$ et $b \equiv c[n] \Rightarrow a \equiv c[n]$.
2. Un entier a est congru modulo n à un et un seul des entiers 0,1,...n-1, qui est le reste dans la division de n par a.
3. La relation de congruence modulo n est compatible avec l'addition, à savoir :

$$a \equiv a'[n] \text{ et } b \equiv b'[n] \Rightarrow a + b \equiv a' + b'[n].$$

4. La relation de congruence modulo n est compatible avec la multiplication, à savoir :

$$a \equiv a'[n] \text{ et } b \equiv b'[n] \Rightarrow a \times b \equiv a' \times b'[n].$$

Démonstration : écrire les définitions ;

Définition 3 *classes d'un entier modulo n*
On appelle classe d'un entier a modulo n, l'ensemble $\bar{a} = \{m \in \mathbb{Z}; m \equiv a[n]\}$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ces n classes (voir prop. 7-2) : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$.

Théorème 8 *le groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$.
– On définit une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ en posant : $\bar{a} + \bar{b} = \overline{a+b}$;

– L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de cette addition est un groupe commutatif ;
– L'application $a \in \mathbb{Z} \to \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupe surjectif dont le noyau est $\mathbb{Z}/n\mathbb{Z}$. On l'appelle morphisme canonique de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration : facile.

Théorème 9 *l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +)$.

– On définit deux lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ en posant :

$$\bar{a} + \bar{b} = \overline{a + b};$$

$$\bar{a} \times \bar{b} = \overline{a \times b};$$

– L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition et de la multiplication ainsi définie est un anneau commutatif ;

– L'application $a \in \mathbb{Z} \to \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ (morphisme canonique) est un morphisme d'anneau surjectif.

Exercice 11 *on se fait la main :*

1. Calculer la somme des éléments (ou des classes) de $\mathbb{Z}/n\mathbb{Z}$;
2. Calculer la somme des carrés des éléments (ou des classes) de $\mathbb{Z}/n\mathbb{Z}$;
3. Calculer $157^{324}, 107^{324}$ dans $\mathbb{Z}/13\mathbb{Z}$.

2.2 Eléments générateurs du groupe (cyclique) $(\mathbb{Z}/n\mathbb{Z},+)$, inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\times)$

Définition 4
• Soit $(G,\star)$ un groupe et F une partie de G. Le **sous-groupe engendré** par F est le plus petit sous groupe contenant F (intersection des sous-groupes contenant F). On note $< F >$ ce sous-groupe de **partie génératrice** F.
• $(G,\star)$ est **monogène** s'il admet un singleton comme partie génératrice.
• $(G,\star)$ est **cyclique** s'il est monogène et fini.

Exercice 12 *exemples de groupes monogènes, cycliques, de générateurs*

1. Soit $a \in \mathbb{Z}$; quel est le sous-groupe engendré par a?
2. Montrer que $(\mathbb{Z},+)$ est monogène, donner ses générateurs.
3. Montrer que $(Z^2,+)$ admet une partie génératrice composée de deux éléments.
4. Montrer que $(\mathbb{Z}^2,+)$ n'est pas monogène. On raisonnera par l'absurde en caractérisant le sous-groupe engendré par un singleton $\{(u,v)\}$.
5. Donner une condition nécessaire et suffisante sur le couple $((a,b),(c,d))$ pour que ce soit une famille génératrice de $\mathbb{Z}^2$.
6. Quels sont les sous-groupes cycliques des groupes $(\mathbb{Z}/8\mathbb{Z}\,,+)$ et $(\mathbb{Z}/5\mathbb{Z}\,,+)$?

Théorème 10 *générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$*
$(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique.
Ses générateurs sont les classes des entiers premiers avec n.
Lorsque n est premier tout élément non nul est générateur.

Démonstration
• $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique puisqu'il est fini et parce que $\{\bar{1}\}$, par exemple, est génératrice.
Recherchons les éléments générateurs.
• Observons tout d'abord que le sous-groupe F engendré par $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$, est $\{\overline{px}/p \in \mathbb{Z}\}$.
$\boxed{\subset}$ On montre par récurrence que $\overline{px} \in F$ pour $p \in \mathbb{N}$:
- $\bar{0} \in F$ qui contient l'élément neutre ;
- $\overline{px} \in F \Rightarrow \overline{px} + \bar{x} = \overline{(p+1)x} \in F$ qui est stable par addition ;
- Pour $p \in Z^-$, on observe que $\overline{px} = -\overline{|p|x} \in F$ qui contient les opposés de ses éléments.
$\boxed{\supset}$ On vérifie sans peine que $\{\overline{px}/p \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, comme il contient $\bar{x}$, il contient F.

• Supposons maintenant que $\bar{x}$ soit générateur de $\mathbb{Z}/n\mathbb{Z}$; F contient alors $\bar{1}$ ce qui signifie :
- Il existe $p \in \mathbb{Z}$ tel que $\overline{px} = \bar{1}$
- Il existe $p \in \mathbb{Z}$ tel que $px \equiv 1[n]$
- Il existe $p \in \mathbb{Z}, q \in \mathbb{Z}$ tel que $px - qn = 1$ et ainsi (par le théorème de Bezout) x et n sont premiers entre eux.
• La réciproque est évidente : si x et n sont premiers entre eux, $\bar{1} \in F$ et donc, comme $\bar{1}$ engendre $\mathbb{Z}/n\mathbb{Z}$, $\bar{x}$ engendre $\mathbb{Z}/n\mathbb{Z}$.

□

Application fondamentale : deux amants se donnent rendez vous toutes les 5 heures. Montrer qu'ils se seront rencontrés à toutes les heures du jour et de la nuit.
indication : ils vivent dans une société relativement permissive ou sont très habiles.

Théorème 11 *l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, .)$
Soit $n \in \mathbb{N}^* \setminus \{1\}$.
– Les éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, .)$ sont les classes des entiers premiers avec n.
– Lorsque n est premier $\mathbb{Z}/n\mathbb{Z}$ est un corps, sinon ce n'est pas même un anneau intègre.

Démonstration : facile et immédiat

Exercice 13 *voir feuille Maple page 11 pour les calculs dans* $\mathbb{Z}/n\mathbb{Z}$

1. Que peut on dire du nombre de solutions de l'équation $x^2 = a$ dans un corps, dans un anneau quelconque ?
   Préciser pour $\mathbb{R}, \mathbb{C}$. Étudier $z^2 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$ ...
   Pour les équations suivantes, regarder si vous pouvez les écrire sous la **forme canonique** avant tout.
2. Résoudre $Z^2 - 10Z + 6 = 0$ dans $\mathbb{Z}/12\mathbb{Z}$
3. Résoudre $Z^2 - 5Z + 6 = 0$ dans $\mathbb{Z}/12\mathbb{Z}$
4. Résoudre $Z^2 - 5Z + 6 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$

Calculs modulo 12

```
> restart;
```

le calcul des congruences

```
> 12 mod 12;
  39 mod 12;
```

$$0$$

$$3$$

```
> Z12Z:=[seq(k, k=0..11)];
```

$$Z12Z := [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]$$

les solutions de Z^2-5*Z+6 =0 dans Z/12Z.

```
> P:= Z -> Z^2-5*Z+6 mod 12:
  map(P, Z12Z);
```

$$[6, 2, 0, 0, 2, 6, 0, 8, 6, 6, 8, 0]$$

les doubles et les carrés

```
> map(x->x+x mod 12,Z12Z);
  map(x->x*x mod 12,Z12Z);
```

$$[0, 2, 4, 6, 8, 10, 0, 2, 4, 6, 8, 10]$$

$$[0, 1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1]$$

Calculs modulo 13

```
> Z13Z:=[seq(k, k=0..12)];
```

$$Z13Z := [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]$$

les solutions de Z^2-5*Z+6 =0 dans Z/13Z.

```
> P:= Z -> Z^2-5*Z+6 mod 13:
  map(P, Z13Z);
```

$$[6, 2, 0, 0, 2, 6, 12, 7, 4, 3, 4, 7, 12]$$

les doubles et les carrés

```
> map(x->x+x mod 13,Z13Z);
  map(x->x*x mod 13,Z13Z);
```

$$[0, 2, 4, 6, 8, 10, 12, 1, 3, 5, 7, 9, 11]$$

$$[0, 1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1]$$

```
>
```

2.3 Le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$

On observera sans peine que l'ensemble des éléments inversibles d'un anneau $(A, +, \times)$ forme un groupe multiplicatif (et qui se confond avec $A\backslash\{0\}$ ssi A est un corps !) ; par exemple
– le groupe des éléments inversibles de $\mathbb{Z}$ est $\{-1, 1\}$;
– le groupe des éléments inversibles de $\mathbb{K}[X]$ est $\mathbb{K}^*$ (constantes non nulles) ;

Théorème 12 *groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$*

1. Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ forment un groupe (noté parfois $(\mathbb{Z}/n\mathbb{Z})^\times$) ;
2. un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible ssi il est premier avec n;
3. un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible ssi c'est un élément générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$;
4. $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier ; dans ce cas, le groupe des inversibles est $\mathbb{Z}/n\mathbb{Z}\backslash\{0\}$;

Exercice 14

1. (a) Expliciter le groupe des inversibles de $\mathbb{Z}/8\mathbb{Z}$ donner la table de ce groupe.
   (b) Est il cyclique ? peut on en donner une partie génératrice ?
   (c) Construire un isomorphisme de groupes entre $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/8\mathbb{Z})^\times$. Est-ce le seul possible ?
2. Expliciter de même le groupe des inversibles de $\mathbb{Z}/12\mathbb{Z}$ et en donner la table. Est il cyclique ? En donner tous les sous-groupes.

Exercice 15 *Mines*
On note U le groupe des inversibles de $\mathbb{Z}/32\mathbb{Z}$.

1. Quel est l'ordre de 5 dans ce groupe ;
2. Donner un groupe additif isomorphe à U.

Exercice 16 *On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ lorsque p est premier.*

1. Combien y a-t-il de carrés dans $\mathbb{F}_p$? Dessiner. Quelle est leur somme ?
2. Déterminer les carrés des éléments de $\mathbb{F}_7$;

Exercice 17 Soient a, b, c trois entiers. On suppose que $a^3 + b^3 + c^3$ est divisible par 7. Montrer qu'il en va de même pour $a\,b\,c$.

Exercice 18 Quels sont les entiers n pour lesquels $7|n^n - 3$?

Exercice 19 *CCP 2012*

1. Quel est l'ordre de 3 dans $\mathbb{Z}/11\mathbb{Z}$? (formulé : *Déterminer le plus petit entier $p \geq 1$ tel que $3^p \equiv 1[11]$*)
2. Démontrer que pour tout entier naturel n, $3^{n+2102} - 9 \times 5^{2n}$ est divisible par 11.

3 Groupes

3.1 Vocabulaire et échauffements

Définition 5 *rappel du vocabulaire de base*

groupe : Soit E un ensemble non vide et $\star$ une loi interne sur E. On dit que $(E, \star)$ est un groupe ssi
- la loi $\star$ est associative ;
- il existe $e \in E$ tel que $\forall x \in E$, $x \star e = e \star x = x$ (on dit que e est élément neutre pour $\star$)
- pour tout $x \in E$ il existe $x' \in E$ tel que $x \star x' = x' \star x = e$, (on dit que x' est inverse ou symétrique de x).

sous-groupe Soit $(E, \star)$ un groupe d'élément neutre e, on dit qu'une partie H de E est un sous groupe de $(E, \star)$ ssi
- H est non vide ;
- pour tout couple (x, y) d'éléments de H, $x \star y^{-1} \in H$.

ordre d'un groupe on appelle ordre d'un groupe fini, le nombre de ses éléments ;

partie génératrice on dit qu'une partie F d'un groupe G, est une partie génératrice de G', sous-groupe de G ssi G' est le plus petit sous-groupe contenant F (ou, voir la proposition ci-dessous, l'intersection des sous-groupes de E contenant F);

groupe monogène c'est un groupe engendré par un de ses éléments

groupe cyclique c'est un groupe monogène fini (voir le théorème 16) ;

générateur a est générateur d'un groupe (nécessairement monogène ou cyclique) si $\{a\}$ est une partie génératrice de ce groupe ; l'ordre d'un élément de G est l'ordre du sous-groupe qu'il engendre ;

morphisme une application $f : (G, \star) \to (H, *)$ est un morphisme de groupe ssi pour tous $(a, b) \in G^2$ on a $f(a \star b) = f(a) * f(b)$;

noyau avec les mêmes notations, le noyau d'un morphisme f est le sous groupe de G formé des antécédents de l'unité de H;

isomorphisme c'est un morphisme bijectif ;

Proposition 13 *propriétés fondamentales*
Soit $(E, *)$ un groupe :

1. E n'a qu'un élément neutre, tout élément possède un unique inverse (à droite ou à gauche) ;
2. les équations $x \star a = b$ et $a \star x = b$ possèdent chacune une solution et une seule ;
3. $\{e\}, E$, une intersection de sous-groupes de E sont des sous-groupes de E.

Théorème 14 Soient $(G, \times)$ et $(H, \star)$ deux groupes et $\phi : G \to H$ un morphisme de $(G, \times)$ dans $(H, \star)$.

1. Le noyau de ϕ est un sev de $(G, \times)$.
2. $\text{Ker}(\phi) = \{e_G\}$ ssi ϕ est injectif.

Démonstration

3.2 Groupes monogènes et cycliques

Définition 6 Soit G un groupe contenant a;
– En notation multiplicative, on définit a^n par récurrence sur $n \in \mathbb{N}$:
$a^0 = e_G$, $a^{n+1} = a^n \star a$, et en posant $a^n = \left(a^{-1}\right)^{|n|}$ lorsque $n \leq 0$.
– En notation additive, on définit $n \times a$ par récurrence sur $n \in \mathbb{N}$:
$0 = e_G$, $(n+1) \times a = (na) + a$, et en posant $n \times a = |n|(-a)$ lorsque $n \leq 0$.

Exercice 20 *exemples de groupes monogènes, cycliques, de générateurs*

1. (a) Montrer que $(\mathbb{Z}, +)$ est monogène, donner ses générateurs.
   (b) Soit $a \in \mathbb{Z}$; quel est le sous-groupe engendré par a?
2. (a) Montrer que $(\mathbb{Z}^2, +)$ n'est pas monogène.
   (b) Donner une condition sur le couple $((a, b), (c, d))$ pour que ce soit une famille génératrice de $\mathbb{Z}^2$.

Théorème 15 *structure des groupes monogènes et cycliques*
Soit $(G, *)$, un groupe et $\omega \in G$.

1. Le sous groupe de G engendré par ω est l'ensemble des puissances $\{\omega^q;\ q \in \mathbb{Z}\}$;
2. Lorsque le groupe engendré par ω est infini, les éléments ω^q, $q \in \mathbb{Z}$, sont tous distincts et l'application $p \in (\mathbb{Z}, +) \to \omega^p \in (G, \star)$ est un isomorphisme de groupe.
3. Lorsque le groupe engendré par ω est fini, de cardinal n, il est est de la forme $\{\omega^0 = e, \omega^1, \omega^2, ..., \omega^{n-1}\}$, et l'on a $\omega^n = e$, n est le plus petit entier strictement positif tel que $\omega^p = e$. On dit alors que $< \omega >$ est un **groupe cyclique.**

Théorème 16 *le même en notations additives*

1. Soit $(G, +)$, un groupe et $\omega \in G$. Le sous groupe de G engendré par a est l'ensemble $\{n.a;\ n \in \mathbb{Z}\})$;
2. Lorsque le groupe engendré par a est infini, les éléments $0, \pm a, \pm 2a, \pm 3a, ... \pm na...$ sont tous distincts et l'application $p \in (\mathbb{Z}, +) \to p\omega \in (G, +)$ est un isomorphisme de groupe.
3. Lorsque le groupe engendré par ω est fini, de cardinal n, il est est de la forme $\{0, \omega, 2\omega, 3\omega, ...(n-1)\omega\}$ avec $n.\omega = 0$; on dit alors que $< \omega >$ est un **groupe cyclique.**

Théorème 17 *racines de l'unité dans* $\mathbb{C}$
• L'ensemble $\mathbb{U}_n$ des racines n^{iemes} de l'unité dans $\mathbb{C}$, muni de la multiplication est un groupe cyclique.
• Ses générateurs (appelés racines primitives de l'unité) sont les éléments $e^{2ip\pi/n}$ où p est premier avec n.

Exercice 21 Calculer

$$\sum_{k=0}^{8} \cos\left(\frac{(2k+1))\pi}{19}\right).$$

Théorème 18 *groupes monogènes et cycliques*
Soit $(G,\star)$, un groupe monogène de générateur $\omega \in G$.

1. Si G est fini de cardinal n, il est de la forme $G = \{\omega^0 = e, \omega^1, ..., \omega^{n-1}\}$, $\omega^n = e_G$ et l'application $\bar{p} \in (\mathbb{Z}/n\mathbb{Z}, +) \to w^p \in (G,\star)$ est bien définie et c'est un isomorphisme de groupe.

Remarque il s'agit ici de compléter les résultats du 16 et de mettre en évidence des isomorphismes.

Exercice 22 Soit $(G,\star)$ un groupe cyclique d'ordre n.

1. Comparer le nombre de générateurs de G et de $\mathbb{Z}/n\mathbb{Z}$;
2. Combien y a-t-il d'isomorphismes de G sur $\mathbb{Z}/n\mathbb{Z}$?
3. Expliciter les isomorphismes de $\mathbb{Z}/6\mathbb{Z}$ sur le groupe des racines sixièmes de l'unité dans $\mathbb{C}$.

Théorème 19 Soit $(G,\star)$ un groupe et $a \in G$.

1. L'application $f : k \in \mathbb{Z} \to a^k \in G$ est un morphisme de groupes ; son image est $\{a^k; k \in \mathbb{Z}\}$.
2. Si $Ker(f) = \{0\}$, $Im(f)$ est monogène infini et isomorphe à $\mathbb{Z}$;
3. Si $Ker(f) = n\mathbb{Z}$, $Im(f)$ est cyclique et isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration

3.3 Théorème de Lagrange - HP mais...

Théorème **20** *un théorème de Lagrange*[2]
Soit G un groupe fini de cardinal n, H un sous-groupe de G. Alors, l'ordre de H est un diviseur de l'ordre de G.

Démonstration avec l'exercice 23 .

Exercice **23** *démonstration du théorème de Lagrange*

1. On considère un groupe fini, G, et H un sous groupe de G. Montrer que si a et b sont des éléments de G,
   – aH et bH sont équipotents (ie : de même cardinal) ;
   – aH et bH sont, soit égaux, soit d'intersection vide.
2. En déduire que si H est un sous-groupe de G, groupe fini, l'ordre de H est un diviseur de l'ordre de G.
   cet énoncé constitue le théorème de Lagrange

3.4 Groupes produits

Théorème **21** *groupe produit*
Soient $(G_1, \star)$ et $(G_2, \times)$ deux groupes. La loi interne définie sur l'ensemble produit $G_1 \times G_2$ par

$$(a_1, a_2) \odot (b_1, b_2) = (a_1 \star b_1, a_2 \times b_2)$$

confère à $G_1 \times G_2$ une structure de groupe. Ce groupe est le **groupe produit** de $(G_1, \star)$ et $(G_2, \times)$.

Exercice **24**

1. Expliciter la table du groupe produit $\mathbb{U}_2 \times \mathbb{U}_2$. S'agit il d'un groupe cyclique ? Quels sont les sous-groupes cycliques de G?
2. Expliciter la table du groupe produit $\mathbb{U}_3 \times \mathbb{U}_2$. S'agit il d'un groupe cyclique ?
3. Explicitez le groupe des isométries du plan qui laissent globalement invariant un triangle équilatéral. Peut on en donner des parties génératrices est il isomorphe au précédent ?

Exercice **25** *groupe produit et groupes cycliques*
On suppose que G_1 et G_2 sont cycliques, donner une partie génératrice de $G_1 \times G_2$; (voir aussi l'exercice 26).
Pour des exemples de groupes produits, voir le théorème chinois (thm 27), les exercices 15... ;

2. ce n'est pas explicitement au programme, mais je préfère que vous l'ayez vu, y compris dans l'optique des concours. Démonstration à connaître pour les oraux *

Exercice 26 *produit de groupes cycliques*

1. Donner un condition nécessaire pour qu'un produit de 2 groupes cycliques d'ordre n et m soit cyclique (étudier un élément $x = (w_1, w_2)$);
2. Montrer que si n et m sont premiers entre eux, le produit de deux groupes cycliques d'ordres respectifs n et m est cyclique.

voir aussi le théorème chinois 27 et l'exercice 27 .

Exercice 27

1. Vérifier que $(\mathbb{Z}/3\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ est un groupe cyclique.
2. Déterminer à un isomorphisme près les groupes commutatifs d'ordre 6.

3.5 Exercices

Exercice 28 *questions brèves :*

1. Soit G un groupe multiplicatif, $a \in G$.

$$\phi : x \in G \to a^{-1}xa \in G,$$

   est il un morphisme, un isomorpisme ?

2. Dans $(\mathbb{Z}^2, +)$, donner une partie génératrice. A quelle condition (CNS) $((a, b), (a', b'))$ est elle génératrice ?

Exercice 29 *partie génératrice à deux éléments*

1. On considère un groupe $(E, \star)$ et a, b deux éléments de E.
   (a) Justifier que le sous-groupe engendré par $\{a, b\}$ est

$$< \{a, b\} >= \left\{ \prod_{k=1}^{N} a^{p_i} b^{q_i};\ \ N \in \mathbb{N}, \forall i \in [1, N], (p_i, q_i) \in \mathbb{Z}^2 \right\}.$$

   Vous expliciterez avec soin l'inverse d'un tel élément. Les choses se simplifient elles lorsque E est commutatif ?

   (b) Illustrations :
      i. Quel est le sous-groupe de $(\mathbb{R}^*, \times)$ engendré par $1/2$ et $1/3$?
      ii. Quel est le sous-groupe du groupe des bijections de $\mathbb{R}*$ dans lui-même engendré par $x \to 1/x$ et $x \to x + 1$?
2. On suppose que chaque G_i possède une partie génératrice formée de 2 éléments. Donner une partie génératrice de $G_1 \times G_2$;
3. Pour le plaisir d'une analogie : si E et F sont deux $\mathbb{K}-$espace vectoriels de dimensions n et m, que dire de la dimension de $E \times F$? (vous définirez ce qui doit l'être)

Exercice 30 *un groupe de matrices*
On considère les endomorphismes de $\mathbb{C}^4$ associés aux matrices

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ -i & 0 & 0 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

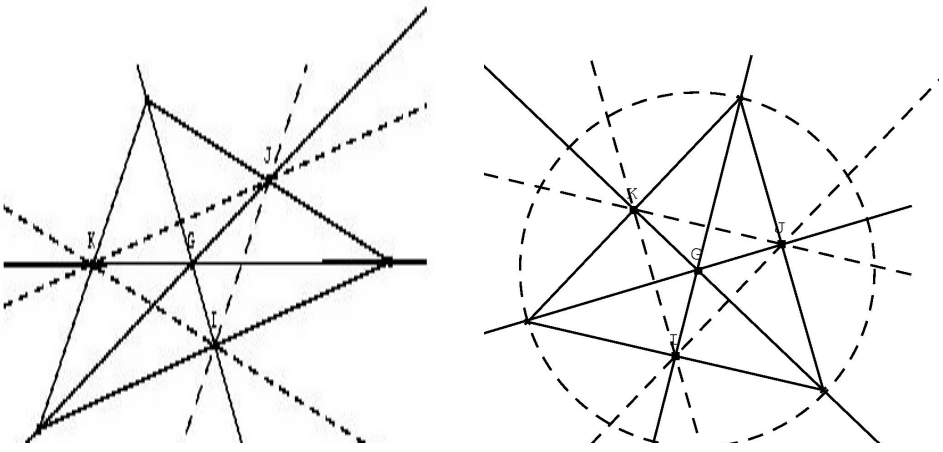
1. Ecrire le carré de la matrice $E = xA + yB + zC + tD$, en déduire des relations remarquables vérifiées par A, B, C, D.
2. Soit $\mathcal{G}$ le sous-groupe de $GL_4(\mathbb{C})$ engendré par $\{A, B, C, D\}$. Montrer que tous ses éléments sont de la forme
$$\pm A^{\alpha_1} B^{\alpha_2} C^{\alpha_3} D^{\alpha_4}$$
avec $\alpha = (\alpha_i) \in \{0, 1\}^4$.
Calculer en particulier l'inverse
$$(A^{\alpha_1} B^{\alpha_2} C^{\alpha_3} D^{\alpha_4})^{-1},$$
sous cette forme.
3. Déterminer le nombre des éléments de $\mathcal{G}$.

Exercice 31 Quel est le plus petit entier n pour lequel il existe un groupe **non commutatif** d'ordre n ?

Exercice 32 *groupes d'isométries laissant une figure invariante*

1. Soit A un ensemble non vide et $\mathcal{B}(A)$ l'ensemble des bijections de A sur lui-même. Montrer que la loi de composition des applications notée $\circ$, est une loi interne sur $\mathcal{B}(A)$ et que $(\mathcal{B}(A), \circ)$ est un groupe (groupe des bijections de A).
2. On rappelle qu'une **application affine** d'un espace euclidien dans lui-même est une application de la forme $f(x) = \phi(x) + u$ où ϕ est linéaire. Une **transformation affine** est une application affine bijective.
   (a) Montrer qu'une application affine conserve le barycentre (après avoir défini cette expression) ;
   (b) Soit f une application affine. Montrer que les trois énoncés suivants sont équivalents :
   - f est une **transformation** affine ;
   - $\phi \in GL(E)$
   - il existe trois points non alignés dont les images par f ne sont pas alignées ;
   - pour toute famille de trois points non alignés, les images par f ne sont pas alignées.

   (c) Montrer que f est une isométrie affine (ie : $||f(x) - f(y)|| = ||x - y||$) ssi $\phi \in O(E)$;
   (d) Montrer que deux applications affines du plan qui coïncident en trois points non alignés sont égales.
3. Soient A, B, C trois points distincts du plan affine euclidien.



triangle quelconque triangle équilatéral

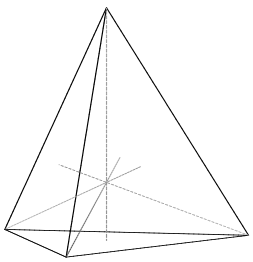
   (a) Montrer que les **transformations** affines qui laissent $T = \{A, B, C\}$ stable (ie : $\Phi(T) \subset T$) forment un groupe qui ne contient aucune translation de vecteur non nul.

(b) Caractériser les éléments de ce groupe en dresser la table, faire apparaître les sous-groupes ; donner une partie génératrice.

(c) Montrer que ce groupe est isomorphe au groupes des permutations de 3 éléments a,b,c.

(d) Montrer que le groupe des isométries qui laissent $T = \{A, B, C\}$ invariant (ie : $\Phi(T) \subset T$) est un sous-groupe du précédent. Lui est il égal ?
On notera : $id, r_1, r_2, s_{(Ag)}, s_{(Bg)}, s_{(Cg)}$... où g est le centre de gravité du triangle, $r_1 = rot(g, 2\pi/3), r_2 = r_1 \circ r_1$, $s_{(Bg)}$ la symétrie orthogonale d'axe (Bg), etc...

4. Idem avec 4 points non coplanaires formant un tétraèdre régulier dans l'espace...



Exercice 33

Soit un entier naturel, $n \geq 2$. On note $\mathcal{A}$ l'ensemble des matrices $M \in \mathrm{Mat}_n(\mathbb{Z})$ pour lesquelles il existe $p \geq 1$ tel que $M^p = I_n$.

1. On donne, pour n=2, $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. S'agit il d'éléments de $\mathcal{A}$? Le groupe multiplicatif qu'elles engendrent est il contenu dans $\mathcal{A}$?
2. (a) Montrer que l'ensemble des polynômes unitaires (ie : de coefficient dominant égal à 1),de degré n, à racines de modules 1 et à coefficients entiers est fini.
   (b) En déduire qu'il existe un entier P tel que pour toute matrice de $\mathcal{A}$, $M^P = I_n$.
3. On se propose de montrer que tout groupe multiplicatif formé d'éléments de $\mathcal{A}$ est fini :
   (a) Soit G un tel groupe. Soit $(A_i)_{1 \leq i \leq p}$ une base de $Vect(G)$ et T l'application de G dans $\mathbb{C}^p$ définie par
   $$T(M) = (Tr(MA_1), ..., Tr(MA_p)).$$
   Prouver que T est injective.
   (b) En déduire que G est fini.

Exercice 34

Soit G un groupe qui n'admet pour sous-groupes que les sous-groupes triviaux : $\{e\}$ et G lui-même.

– Montrer que G est monogène ;
– Montrer que G est cyclique (monogène et fini) ;
– Montrer que Card(G) est premier ou égal à 1.

Exercice 35 ** * loi associative*
Soit E un ensemble fini muni d'une loi interne associative notée T. Démontrer qu'il existe un élément de E au moins tel que $zTz = z$.
voir corrigé en 9.2

Exercice 36
On considère un groupe G tel que pout tout $x \in G, x^2 = e$.

1. Montrer que G est commutatif (considérer $(xy)(xy)...$)
2. Soit H un sous-groupe de G et $x \notin H$. Montrer que le sous-groupe engendré par $H \cup \{x\}$ est de cardinal $2CardH$.
3. En déduire que Card G est une puissance de 2.

4 Anneaux et corps, généralités, notion d'idéal

Définition 7 *anneaux commutatifs, corps et idéaux*

1. Un ensemble A muni de deux LCI notées $+$ et $\times$ est un **anneau** ssi
   – $(A,+)$ est un groupe commutatif ;
   – la loi $\times$ est distributive par rapport à $+$:
   – $(a+b)\times c = a\times c + b\times c,\ c\times(a+b) = c\times a + c\times b$;
   – A possède un élément neutre pour $\times$;
   On dit que A est un **anneau d'intégrité si,** de plus :
   $$xy = 0 \Rightarrow x = 0 \text{ ou } y = 0;$$
2. On dit que l'anneau $(A,+,\times)$ est un **corps** ssi tout élément son nul de A est inversible (pour $\times$) (c'est alors un anneau d'intégrité) ;
3. Une partie non vide de $I \subset A$, est un **sous-anneau** si c'est un sous-groupe de $(A,+)$ qui est aussi stable pour la loi $\times$ et contient l'élément neutre.
4. Soient $(A,+,\times)$ et $(B,+,\star)$ deux anneaux ; on dit qu'une application ϕ de A vers B est un **morphisme d'anneaux** lorsque
   – c'est un morphisme de groupes de $(A,+)$ vers $(B,+)$;
   – on a la formule : $\phi(a\times b) = \phi(a)\star\phi(b)$;
5. **produit de deux anneaux** $(A,+,\times)$ **et** $(B,+,\times)$, c'est l'anneau $(A\times B,+,\times)$ dont les opérations sont définies par
   $$(a,b)+(a',b') = (a+a',b+b') \text{ et } (a,b)\times(a',b') = (aa',bb');$$
6. Dans un anneau d'intégrité commutatif, on définit une relation de **divisibilité** en posant :
   $$a|b \Leftrightarrow \exists d\in A,\ b = da \Leftrightarrow bA \subset aA;$$

Exercice 37 *brèves (à faire seul(e))*

1. combien l'équation $x^2 = 1$ a-t-elle de solutions dans un corps, dans un anneau ?
2. le produit de deux corps est un anneau, peut il être un corps ?

Définition 8 *idéal*
Soit A un anneau de lois $+$ et $\times$. Un idéal de A est une partie $\mathcal{I}$, de A est un sous-groupe de $(A,+)$ tel que
$$\forall x\in A,\ \forall j\in\mathcal{I},\ x\times j\in\mathcal{I} \text{ et } j\times x\in\mathcal{I}.$$

Exercice 38 *exemples*

1. les polynômes de la forme $PA+BQ$, (A,B) donné et (P,Q) décrivant $\mathbb{K}[X]^2$, dans $A = \mathbb{K}[X]$.
2. les fonctions de E ensemble quelconque, dans $\mathbb{R}$ nulles sur une partie donnée de E, dans $A = \mathcal{F}(E,\mathbb{R})$.
3. les multiples de a dans $\mathbb{Z}$...

Exercice 39 *exemples d'anneaux et d'idéaux, brèves*
On sait que $(\mathbb{Z},+,\times),(\mathbb{K}[X],+,\times)$, $(\mathcal{L}(E),+,\circ)$, l'ensemble $\mathcal{F}(X,A)$ (des fonctions de X vers l'anneau A) muni de l'addition et de la multiplication des fonctions, sont des anneaux...

1. Quels sont les anneaux d'intégrité parmi eux ?
2. Vérifier que dans $\mathcal{F}(X,A)$ l'ensemble des fonctions nulles sur $U \subset X$ est un idéal ;
3. Soit q un naturel non carré. On note $\mathbb{Z}[\sqrt{q}], \mathbb{Q}[\sqrt{q}]$, les éléments de la forme $a+b\sqrt{q}$, avec a et b dans $\mathbb{Z}$ ou $\mathbb{Q}$ respectivement. Anneaux, corps ?
4. Donner des exemples de sous-anneaux qui ne sont pas des idéaux ;
5. Quels sont les idéaux d'un corps ?
6. Soit A un anneau et $a_1,...,a_n \in A$, montrer que l'ensemble des éléments de la forme

$$a_1u_1 + ... + a_nu_n,$$

   est, un idéal et que c'est l'intersection de tous les idéaux contenant les a_i.
7. Ordonner les idéaux de $\mathbb{Z}$ que sont $\{0\},\mathbb{Z},2\mathbb{Z},3\mathbb{Z},4\mathbb{Z},5\mathbb{Z},6\mathbb{Z},8\mathbb{Z},9\mathbb{Z},12\mathbb{Z},15\mathbb{Z}$...
8. Préciser $18\mathbb{Z} \cap 12\mathbb{Z}$, $14\mathbb{Z} \cap 21\mathbb{Z}$.

Théorème 22 Dans un anneau A, une intersection d'idéaux est un idéal de A;

Démonstration immédiat ;

Définition 9

si U est une partie non vide de A, on appelle idéal engendré par U l'intersection des idéaux de A contenant U;

5 L'anneau $\mathbb{Z}/n\mathbb{Z}$; compléments

5.1 Idéaux de $\mathbb{Z}$, arithmétique

Théorème 23 *sous-anneaux et idéaux de* $\mathbb{Z}$

1. Les sous-groupes de $\mathbb{Z}$ sont les parties $a\mathbb{Z}$, $a \in \mathbb{Z}$.
2. Les idéaux de $\mathbb{Z}$ sont ses sous-anneaux ;
3. $a|b$ ssi $b\mathbb{Z} \subset a\mathbb{Z}$;
4. L'intersection des idéaux $a\mathbb{Z}$ et $b\mathbb{Z}$ est l'idéal $m\mathbb{Z}$ où m est le ppcm de a et de b;
5. Soient a et b deux entiers non nuls, l'idéal engendré par a et b est l'ensemble

$$\{au + bv;\ (u,v) \in \mathbb{Z}^2\} = d\mathbb{Z}$$

   où $d = pgcd(a,b)$ est le plus grand diviseur commun de a et de b.

Démonstration seraient-ce immédiatetés ?

Théorème 24 *théorème de Bezout*
Soient a et b deux entiers non nuls. Les propositions suivantes sont équivalentes :

1. a et b sont premiers entre eux,
2. l'idéal $\{au + bv;\ (u, v) \in \mathbb{Z}^2\}$ est égal à $\mathbb{Z}$,
3. il existe deux entiers u et v tels que

$$au + bv = 1.$$

Théorème 25 *théorème de Gauss*
Si deux entiers a et b sont premiers entre eux, alors $a \,|\, b\,x \Rightarrow a \,|\, x$.

Exercice 40 *questions de divisibilité*
On suppose p premier.

1. Montrer que, si $0 < i < p$, les coefficients binomiaux $\binom{p}{i}$, sont des multiples de p; qu'en est il si p n'est pas premier ?
2. Soient a et b des entiers. Montrer que $(a + b)^p \equiv a^p + b^p[p]$;
3. Montrer que si $a \in \mathbb{N}$, $a^p \equiv a[p]$ (petit théorème de Fermat)
4. Soient p, un nombre premier impair, $n \in \mathbb{N}$ et $a \in A$. . Démontrer les propriétés suivantes :
   - $(1 + pa)^{p^n} \equiv 1 + p^{n+1}a[p^{n+2}]$
   - $(1 + p^a)^p \equiv 1 + p^{n+1}a[p^{n+2}]$
     (cette dernière par récurrence sur n)

Exercice 41 *mines 2006*

1. Caractériser les matrices de $\mathcal{M}_n(\mathbb{Z})$ inversibles et dont l'inverse est dans $\mathcal{M}_n(\mathbb{Z})$.
2. On suppose que A et B sont deux matrices de $\mathcal{M}_2(\mathbb{Z})$ dont les déterminants sont premiers entre eux. Démontrer qu'il existe deux matrices de $\mathcal{M}_2(\mathbb{Z})$ telles que $AU + BV = I_2$.
   (corrigé dans le poly révisions oraux).

5.2 Caractéristique d'un corps

Théorème 26
Soit $(A, +, \times)$ un anneau intègre (ou un corps) dont l'élément neutre pour la multiplication est noté 1_A.

– Il existe un morphisme d'anneaux, non nul, et un seul $\phi : (\mathbb{Z}, +, \times) \to (A, +, \times)$;
– Le noyau de ϕ est un sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$. Lorsque ce sous-groupe n'est pas réduit à $\{0\}$, il existe un morphisme **injectif** $\psi : \mathbb{Z}/n\mathbb{Z} \to A$ et un seul tel que $\phi = \psi \circ m$ où m est le morphisme canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, ce que l'on aime à résumer par le diagramme :

$$\begin{array}{ccc} & \phi & \\ \mathbb{Z} & \to & A \\ & m \searrow & \uparrow \quad \psi \\ & & \mathbb{Z}/n\mathbb{Z} \end{array}$$

– Lorsque A est un corps, l'entier n est premier ou nul, on dit que c'est la **caractéristique du corps** A.

Démonstration

– Construction de ϕ :
Analyse on commence par prouver que si ϕ est un morphisme d'anneaux non nul, $\phi(0) = 0_A$ et $\phi(1) = 1_A$. On en déduit $\phi(n) = n1_A$ pour $n \in \mathbb{N}$ (avec la convention $Ox = 0_A, (n+1)x = nx + x$, pour $n \in \mathbb{N}x \in A$, puis $nx = -|n|x$ pour $n \in \mathbb{Z}^-$). Cela prouve l'unicicité de ϕ.
Synthèse on vérifie sans peine que l'application définie par $\phi(n) = n1_A,\ n \in \mathbb{Z}$, est un morphisme d'anneaux (récurrences).
– Le noyau de ϕ est un sous-groupe de $\mathbb{Z}$, de la forme $n\mathbb{Z}$; si $n \neq 0$, on s'assure que

$$x \equiv x'[n] \Rightarrow \phi(x) = \phi(x'),$$

ce qui permet de définir **l'application** ψ en posant

$$\psi(\bar{x}) = \phi(x).$$

– On prouve ensuite que ψ est un morphisme d'anneaux, l'injectivité est immédiate puisque

$$\psi(\bar{x}) = 0 \Leftrightarrow \phi(x) = 0 \Leftrightarrow x \in n\mathbb{Z}...$$

– **Supposons maintenant que A est un corps :**
si $\bar{x} \neq \bar{0}$, $\psi(\bar{x}) \neq 0_A$, cet élément est donc inversible dans A. En particulier pour $a = 1, ...n-1$ on a :

$$\psi(\bar{a}\bar{x}) = \psi(\bar{a})\psi(\bar{x}) \neq 0_A.$$

$\mathbb{Z}/n\mathbb{Z}$ ne contient donc pas de diviseurs de 0, n est premier.

Exemples
• le corps $\mathbb{Z}/p\mathbb{Z}$ lorsque p est premier est de caractéristique p;
• $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont de caractéristique nulle ;
• il existe des corps de caractéristique p (premier) autres que $\mathbb{Z}/p\mathbb{Z}$; voir par exemple l'exercice 48.

Exercice 42

1. Montrer que dans un corps commutatif de caractéristique p, $(x+y)^p = x^p + y^p$;
2. Montrer que si p est premier et $a \in \mathbb{N}$, $a^p \equiv a[p]$; comparer à la résolution précédente.

Exercice 43 *nombre d'éléments d'un corps fini*
Soit $\mathbb{F}_q$ un corps fini ayant q éléments.

1. Montrer que F_q est un corps de caractéristique p non nulle ;
2. Définir sur F_q une structure de $\mathbb{Z}/p\mathbb{Z}-$espace vectoriel ;
3. Montrer que q est une puissance de p.

voir l'exercice 48.

5.3 L'indicatrice d'Euler

Théorème 27 *Soient $n_1, n_2, ..., n_p$ des entiers > 0,* **premiers entre eux deux à deux,** *de produit égal à n.*
– *Les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_i \mathbb{Z}/n_i\mathbb{Z}$ sont isomorphes.*
– *Les groupes commutatifs $\mathbb{Z}/n\mathbb{Z}^\times$ et $\prod_i (\mathbb{Z}/n_i\mathbb{Z})^\times$ sont isomorphes.*

Exercice 44 *démonstrations du théorème chinois*

1. **Première preuve : On considère m et n premiers entre eux** on considère $\phi : x \in \mathbb{Z} \to (\bar{x}^{[n]}, \bar{x}^{[m]}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
   (a) Vérifier que ϕ est un morphisme d'anneaux et déterminer son noyau ;
   (b) Montrer qu'il existe un isomorphisme d'anneau de $\mathbb{Z}/nm\mathbb{Z}$ dans l'anneau produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$;
   (c) Conclure.
2. Deuxième preuve : On considère l'application $\psi : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ définie par $\psi(\bar{x}^{[nm]}) = (\bar{x}^{[n]}, \bar{x}^{[m]})$;
   (a) Assurez vous que ψ est correctement définie, que c'est un homomorphisme d'anneaux ; le fait que pgcd(n,m)=1 intervient il ?
   (b) Montrer que ψ est un isomorphisme et dire comment on calcule ψ^{-1}.
3. Résoudre les systèmes de congruences suivants :

$$\begin{cases} x & \equiv 2[12] \\ x & \equiv 7[25] \end{cases} \tag{5.1}$$

$$\begin{cases} x & \equiv 4[15] \\ x & \equiv 7[32] \end{cases} \tag{5.2}$$

On a ainsi prouvé le théorème 27

Définition 10 *indicatrice d'Euler*
On appelle indicatrice d'Euler l'application $\phi : \mathbb{N} \to \mathbb{N}$ définie par

$$\phi(n) = Card\left((\mathbb{Z}/n\mathbb{Z})^\times\right).$$

C'est aussi le nombre des entiers $1 \leq p \leq n$, premiers avec n.

Théorème 28 *propriétés de l'indicatrice d'Euler*
– Si p est premier, $\phi(p) = p - 1$ et $\phi(p^s) = p^{s-1}(p-1)$;
– si m et n sont premiers entre eux, $\phi(mn) = \phi(m)\phi(n)$;
– pour un naturel n dont la décomposition en facteurs premier est $n = \prod_i p_i^{s_i}$, on a

$$\phi(n) = n\prod_i (1 - 1/p_i).$$

Démonstrations
– pour $n = p$ ou $n = p^\alpha$, c'est chose facile
– pour n quelconque on propose en exercice deux démonstrations ; la seconde ne faisant pas appel au théorème chinois est plus conforme au programme :

avec le théorème chinois

1. Pour montrer que ϕ est multiplicative, repérer les inversibles de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ lorsque n et m sont premiers entres eux et comparer aux inversibles de $\mathbb{Z}/nm\mathbb{Z}$;
2. en déduire la formule générale

sans le théorème chinois démonstration combinatoire

1. Vous savez compléter la formule de dénombrement $Card(A \cup B) = ...$ Donner la formule correspondant à la réunion de s parties.
2. On considère $n = \prod_{i=1}^{d} p_i^{\alpha_i}$. Combien y a-t-il d'entiers compris entre 1 et $n-1$ ayant $p_{i_1} \times p_{i_2} ... \times p_{i_s}$ comme facteur commun avec n?
3. Calculer $\phi(n)$;
4. Déduire de la formule explicite que ϕ est multiplicative.

Exercice 45 *théorème d'Euler*

1. Quelles sont les valeurs de r^7 dans $\mathbb{Z}/7\mathbb{Z}$, de $r^{\phi(n)}$ dans $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$?
2. On se propose de généraliser ce qui vient d'être observé. Pour cela considérons $\bar{a}$ un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ et l'application

$$h : \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times \to \bar{a}\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$$

où $(\mathbb{Z}/n\mathbb{Z})^\times$ désigne l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
   (a) Montrer que h est une bijection de $(\mathbb{Z}/n\mathbb{Z})^\times$ dans lui-même.
   (b) Calculer de deux façons le produit

$$\prod_{\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times} h(\bar{x})$$

et en déduire que $\bar{a}^{\phi(n)} = \bar{1}$ (théorème d'Euler).

5.4 Exercices

Exercice 46 *théorème de Wilson*

1. Soit p un nombre premier.
   (a) Montrer que $(p-1)! \equiv -1\ [p]$;
   (b) Montrer que si $p \equiv 1[4]$, $(p-1)! = -1$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$
   (c) Qu'en est il si $p \equiv 1[4]$?
2. On suppose que n n'est pas premier, que vaut $(n-1)!\ [n]$?

Exercice 47 *TPE-2003 (deux morceaux de planches)*

1. Résoudre dans $\mathbb{Z}/17\mathbb{Z}$, l'équation $x^2 - 3x + k = 0$; Discuter suivant la valeur de k.
2. – Reste de la DE de 4851^{203} par 5 ;
   – Résoudre dans $\mathbb{Z}/143\mathbb{Z}$, l'équation $x^2 - 3x + 2 = 0$;

Exercice 48 *un corps de caractéristique 5 ayant 25 éléments ;*
On note $\mathbb{F}_5$ le corps $\mathbb{Z}/5\mathbb{Z}$.

1. Écrire la table de multiplication de ce corps ; quels sont ses carrés ? les formules de Cramer y sont elles valides ?
2. On suppose qu'il existe un sur-corps commutatif de $\mathbb{F}_5$ contenant un élément q tel que $q^2 = 2$. Calculer $(a + bq)(a' + b'q)$ dans ce sur-corps.
3. On définit sur $\mathbb{F}_5 \times \mathbb{F}_5$ une addition et une multiplication en posant :

$$(a, b) + (a', b') = (a + a', b + b') \text{ et } (a, b) \times (a', b') = (aa' + 2bb', ab' + a'b);$$

   (a) Vérifier que muni de ces deux lois $\mathbb{F}_5 \times \mathbb{F}_5$ est un corps de caractéristique 5 ;
   (b) Montrer que $\mathbb{F}_5$ est isomorphe à un sous-corps de $\mathbb{F}_5 \times \mathbb{F}_5$.

   Cela vous rappelle-t-il quelque chose ?

Exercice 49 *polynômes cyclotomiques*
On rappelle que le groupe multiplicatif $(\mathbb{U}_n, \times)$ des racines $n^{ième}$ de l'unité dans le corps des complexes est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$, qu'une racine primitive $n^{ième}$ de l'unité est un générateur de $\mathbb{U}_n$, à savoir, un élément de la forme $e^{2ik\pi/n}$, avec k premier avec n.
On appelle **polynôme cyclotomique** d'ordre n le polynôme

$$\Phi_n(X) = \prod_{\zeta \text{racine primitive } n^{ième}} (X - \zeta) = \prod_{k \in \mathbb{Z}/n\mathbb{Z}^\times} \left(X - e^{2ik\pi/n}\right).$$

1. Quel est le degré de $\Phi_n(X)$?
2. Calculer $\Phi_p(X)$, puis $\Phi_{p^s}(X)$, lorsque p est premier.
3. Calculer les polynômes cyclotomiques d'ordres 1, 2, 3, 4, 5, 6. Vérifier que $X^6 - 1$ est le produit des Φ_k avec $k|6$.
4. Généraliser ce résultat et en déduire que l'indicateur d'Euler vérifie

$$\phi(n) = \sum_{d|n} \phi(d).$$

Exercice 50 *codage et décodage RSA*

On rappelle que si $n = \prod p_i^{\alpha_i}$, les entiers p_i étant premiers et distincts, le nombre des entiers premiers avec n compris entre 1 et n est

$$\phi(n) = n \prod \left(1 - \frac{1}{p_i}\right).$$

1. (a) Vérifier que pour tout élément inversible $\bar{x}$, de l'anneau $\mathbb{Z}/12\mathbb{Z}$, on a $\bar{x}^{\phi(n)} = \bar{1}$.
   (b) Qu'en est il dans $\mathbb{Z}/13\mathbb{Z}$?
2. On se propose de généraliser ce qui vient d'être observé. Pour cela considérons $\bar{a}$ un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ et l'application

   $$h : \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times \to \bar{a}\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times$$

   où $(\mathbb{Z}/n\mathbb{Z})^\times$ désigne l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.
   (a) Montrer que h est une bijection de $(\mathbb{Z}/n\mathbb{Z})^\times$ dans lui-même.
   (b) Calculer de deux façons le produit

   $$\prod_{\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times} h(\bar{x})$$

   et en déduire que $\bar{a}^{\phi(n)} = \bar{1}$ (théorème d'Euler).
3. Dans ce qui suit, p et q sont deux premiers positifs distincts et $n = pq$.
   (a) Soit $d \in \mathbb{N}$, à quelle condition existe-t-il $e \in \mathbb{N}$ tel que $\bar{d}\bar{e} = \bar{1}$ dans $\mathbb{Z}/w\mathbb{Z}$ où $w = \phi(n)$?

   On suppose désormais que d et e sont inverses dans $\mathbb{Z}/w\mathbb{Z}$ et on définit deux applications de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même [3] :

   $$cod : \bar{m} \in \mathbb{Z}/n\mathbb{Z} \to \bar{m}^e \in \mathbb{Z}/n\mathbb{Z},$$

   $$dec : \bar{c} \in \mathbb{Z}/n\mathbb{Z} \to \bar{c}^d \in \mathbb{Z}/n\mathbb{Z}.$$

   (b) On suppose que $\bar{m}$ est inversible (dans $\mathbb{Z}/n\mathbb{Z}$). Calculer $dec \circ cod(\bar{m})$.
   (c) Montrer que les entiers m compris entre 1 et $n-1$ et tels que $\bar{m}$ ne soit pas inversible dans $\mathbb{Z}/n\mathbb{Z}$ sont de la forme xp^s ou xq^s avec x premier avec n, $s \in \mathbb{N}^*$.
   (d) On suppose que $m = p^s, s \geq 1$.
   Montrer que $m^{de} - m \equiv 0[p]$ et $m^{de} - m \equiv 0[q]$. En déduire que $dec \circ cod(\bar{m}) = \bar{m}$.
   (e) On suppose que $m = xp^s$ où x est premier avec n, et que $1 \leq m \leq n-1$; Calculer $dec \circ cod(\bar{m})$.
   (f) En déduire $dec \circ cod$.

corrigé en 9.2 ;
pour une mise en œuvre, voir le TD MAPLE proposé en section (59).

3. on ne confondra pas les classes modulo n et les classes modulo w

6 A propos des polynômes

6.1 Division euclidienne des polynômes

Théorème 29
Soit $\mathbb{K}$ un corps. L'anneau des polynômes sur $\mathbb{K}$ est un anneau d'intégrité sur lequel est définie une division euclidienne :

$$\phi : (A(X), B(X)) \in \mathbb{K}[X] \times (\mathbb{K}[X]/\{0\} \to (Q(X), R(X)) \in K[X] \times K[X]$$

où le couple $(Q(X), R(X))$ est l'unique couple vérifiant

$$A(X) = Q(X)B(X) + R(X) \text{ avec } degR(X) < deqB(X).$$

6.2 Racines et coefficients

On rappelle les relations liant les racines d'un polynôme à ses coefficients : si

$$P(X) = \sum_{i=0}^{n} a_i X^i = a_n \prod_{i=1}^{n} (X - \alpha_i) \in \mathbb{K}[X]$$

est un polynôme scindé sur $\mathbb{K}$, alors

$$\begin{cases} \sigma_1 & = \sum_i \alpha_i & = -\dfrac{a_{n-1}}{a_n}, \\ \sigma_2 & = \sum_{1 \le i < j \le n} \alpha_i \alpha_j & = \dfrac{a_{n-2}}{a_n}, \\ \vdots & \vdots & \vdots \\ \sigma_k & = \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} \alpha_{i_1} \ldots \alpha_{i_k} & = (-1)^k \dfrac{a_{n-k}}{a_n}, \\ \vdots & \vdots & \vdots \\ \sigma_n & = \alpha_1 \ldots \alpha_n & = (-1)^n \dfrac{a_0}{a_n}. \end{cases}$$

Exercice 51 *méthode de Souriau et Faedev*
On désigne ici par $\mathcal{P}_k(\Lambda)$, l'ensemble des k-parties de $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$, pour $1 \le k \le n$, et des variables formelles $\lambda_1, \ldots, \lambda_n$. On définit comme à l'accoutumée les fonctions symétriques

$$\sigma_k = \sum_{\nu \in \mathcal{P}_k(\Lambda)} \lambda_{\nu_1} \ldots \lambda_{\nu_k} \text{ et } S_k = \sum_{i=1}^{n} \lambda_i^k.$$

1. Exprimer, lorsque $n = 4$, $\sigma_1, \sigma_2, \sigma_3$ en fonction des S_i, $1 \le i \le 3$.

2. Soit A une matrice carrée d'ordre 4, à coefficients complexes, on définit une suite $(X_k)_k$ en posant :

$$\begin{cases} X_0 = A \\ X_{k+1} = A\left(X_k - \dfrac{1}{k+1}\mathrm{Tr}(X_k)I_4\right). \end{cases}$$

Montrer que la suite est stationnaire (ie : constante à partir d'un certain rang) et montrer que l'on peut exprimer le polynôme caractéristique de A en fonction des premiers termes de la suite $(X_k)_k$.
Que dire de σ_4?

3. On donne $A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & -1 & 1 & 0 \\ 2 & -2 & 0 & 0 \\ 0 & 1 & 2 & 3 \end{bmatrix}$, calculer son polynôme caractéristique sans utiliser de formule directe de calcul de déterminant.

Exercice 52 *polynômes de* $\mathbb{Z}[X]$

1. On considère la matrice $A \in \mathcal{M}_n(\mathbb{Z})$, définie par

$$A = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & 0 & -a_{n-2} \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}.$$

Calculer le polynôme caractéristique de A.

2. (a) Factoriser dans $\mathbb{Z}[X]$ et dans $\mathbb{C}[X]$ le polynôme $X^3 - 1$. On note α_k ses racines dans $\mathbb{C}$ et $R(X) = X^2 + 2X + 4$. Calculer le polynôme

$$\prod_{k=1}^{3}(X - R(\alpha_k)).$$

(b) Donner une matrice M dont $P(X)$ est le polynôme caractéristique. Que peut on dire de $R(M)$?

3. Soit P un polynôme de $\mathbb{Z}_n[X]$ se factorisant sur $\mathbb{C}$ en

$$P(X) = \prod_{k=1}^{n}(X - \alpha_k).$$

Montrer que pour tout polynôme $R(X) \in \mathbb{Z}[X]$, le polynôme

$$S(X) = \prod_{k=1}^{n}(X - R(\alpha_k))$$

est lui aussi un polynôme à coefficients entiers.

Exercice 53

Soient f et g deux polynômes de $\mathbb{C}[X]$, de degrés respectifs $p \geq 1$ et $q \geq 1$.

1. Montrer que f et g ont une racine commune si et seulement si :
   il existe deux polynômes *non nuls*, A et B tels que

$$\begin{cases} (i)\ \deg(A) \leq q-1 \\ (ii)\ \deg(B) \leq p-1 \\ (iii)\ A\,f + B\,g = 0 \end{cases}$$

2. On considère l'application

$$\phi : (A,B) \in \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X] \to A\,f + B\,g \in \mathbb{C}_{p+q-1}[X]$$

   Justifier que ϕ est bijective si et seulement si f et g n'ont aucune racine commune.

3. On considère : $f(X) = aX^2 + X - 1,\ g(X) = aX^3 + aX^2 + 1$. Écrire la matrice de ϕ dans une base bien choisie. Donner les valeurs de a pour lesquelles ces polynômes ont une même racine.

correction

1. $\Rightarrow$: On suppose que f et g ont une racine commune. On factorise dans $\mathbb{C}$: $f(X) = a\prod(X-\alpha_i),\ g(X) = b\prod(X-\beta_j)$.
   On note $\alpha_{i_0} = \beta_{j_0}$ une racine commune. On pose

$$A = \frac{g}{X-\beta_{j_0}},\ B = \frac{-f}{X-\alpha_{i_0}}.$$

   $\Leftarrow$: on suppose qu'il existe $A,\ B$ tels que (i),(ii) et $A\,f + B\,g = 0$.

2. ϕ est linéaire les espaces de départ et d'arrivée ont la même dimension : $p+q$. ϕ est bijective ssi $\mathrm{Ker}(\phi) = \{0\}$...

3. On choisit comme bases :

$$\mathcal{B} = \{(X^i, 0); 0 \leq i \leq q-1\} \cup \{(0, X^j); 0 \leq j \leq p-1\},$$

   et la base canonique.
   La matrice est alors, pour $a \neq 0$: $\begin{bmatrix} a & 0 & 0 & a & 0 \\ 1 & a & 0 & a & a \\ -1 & 1 & a & 0 & a \\ 0 & -1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 \end{bmatrix}$ et son déterminant est :
   $a\left(4\,a^2 - 4\,a - 1\right)$, et a pour racines :

$$1/2 - 1/2\,\sqrt{2}, 0, 1/2\,\sqrt{2} + 1/2.$$

   Le cas $a = 0$, conduit à des polynômes de degrés inférieurs dont $g = 1$(voir feuille de travail Maple). Dans les deux autres cas f est du second degré une de ses deux racines est racine de g.

Exercice 54 *majoration des racines ou des coefficients*

1. Montrer que l'ensemble des polynômes unitaires (ie : de coefficient dominant égal à 1),de degré n, à racines de modules 1 et à coefficients entiers est fini.
2. Soit $F(X) = X^n + a_{n-1}X^{n-1} + ... + a_{n-k}X^{n-k} + ... + a_0$, un polynôme à coefficients complexes.
   (a) Montrer que si α est une racine de F, alors
   $$|\alpha| \leq 2 \max_k |a_{n-k}|^{1/k}$$
   (b) Montrer que, si α est une racine de F, alors
   $$|\alpha| \leq \frac{1}{2^{1/n} - 1} \max_k \frac{|a_{n-k}|}{\binom{n}{k}^{1/k}}$$
   indication : calculer $(|\alpha| + \rho)^n$, choisir un majorant de ρ.
   (c) On suppose que F a des coefficients entiers et que
   $$G(X) = b_q X^q + b_{q-1}X^{q-1} + ... + b_0,$$
   divise F. Montrer que si les racines de F, vérifient $|\alpha| \leq R$, alors, les coefficients de G vérifient :
   $$|b_j| \leq sup\binom{q}{k} R^k.$$

6.3 Idéaux de $\mathbb{K}[X]$

Théorème 30
Dans $\mathbb{K}[X]$, tout idéal $\mathcal{I}$ est de la forme $\mathcal{I} = G(X) \times \mathbb{K}[X]$. On dit que G est un générateur de l'idéal $\mathcal{I}$ et on note $\mathcal{I} = (G(X))$.
Le polynôme $G(X)$ est unique à une constante multiplicative prés, ie :

$$G(X) \times \mathbb{K}[X] = H(X) \times \mathbb{K}[X] \Rightarrow (\exists \alpha \in \mathbb{K},\ G = \alpha H).$$

Démonstration division euclidienne et degré du reste...

Définition 11 – on appelle pgcd de deux polynômes non nuls $A(X)$ et $B(X)$ un générateur de l'idéal $(A(X)) + (B(X))$;
– on appelle ppcm de deux polynômes non nuls $A(X)$ et $B(X)$ un générateur de l'idéal $(A(X)) \cap (B(X))$;

Théorème 31 *algorithme d'Euclide pour les polynômes* Soient A et B deux polynômes de $\mathbb{K}[X]$.
On considère la suite définie par :
$R_0 = A,\ R_1 = B$, et, tant que $R_i \neq 0$, $R_{i-1} = R_i q_i + R_{i+1}$ avec $degR_{i+1} < degR_i$. Cette suite est finie, son dernier terme est nul et le dernier non nul est le pgcd de A et B :

$$R_N = pgdd(A, B) = u_N A + v_N B$$

Démonstration pas de différence avec le cas des entiers ;

6.4 Le théorème de Bezout

Définition 12
Soient A et B deux polynômes, on dit que A et B sont premiers entre eux ssi leurs seuls diviseurs communs sont les constantes.

Exercice 55 *exemples*
Montrer que deux polynômes scindés sont premiers entre eux ssi ils n'ont pas de racine commune ;

Théorème 32 Soient A et B deux polynômes. Les propositions suivantes sont équivalentes :

1. A et B sont premiers entre eux,
2. l'idéal $\{AP + BQ;\ (P, Q) \in \mathbb{K}[X]^2\}$ est égal à $\mathbb{K}[X]$,

3. il existe deux polynômes P et Q tels que
$$AP + BQ = 1.$$

Démonstration
– $1 \Rightarrow 2$: A et B premiers entre eux, nous supposerons.
L'idéal $\mathcal{I} = \{AP + BQ; (P, Q) \in \mathbb{K}[X]\}$ est de la forme $\mathcal{I} = D \times \mathbb{K}[X]$. D divise donc A comme B qui sont éléments de $\mathcal{I}$ (remplacer P et Q comme il se doit...). D est donc une constante non nulle, et $\{AP + BQ;\ (P, Q) \in \mathbb{K}[X]^2\} = \mathbb{K}[X]$.
– $2 \Rightarrow 3$: comme $1 \in \mathcal{I}$, il existe des polynômes tels que $AU + BV = 1$;
– $3 \Rightarrow 1$: $AP + BQ = 1$, nous supposerons :
Si D divise à la fois A et B, $AP + BQ = 1$, il divisera, et donc scalaire il sera.

Théorème 33 *lemme de Gauss*
si A et B sont des polynômes premiers entre eux, alors pour tout polynôme C,
$$A|BC \Rightarrow A|C.$$

Démonstration

Remarque : en arithmétique des entiers, on a énoncé de la même façon :
• tout idéal de $\mathbb{Z}$ est de la forme $\mathcal{I} = a\mathbb{Z}$.

• a et b sont premiers entre eux ssi il existe u et v tels que
$$au + bv = 1.$$
• si a et b sont des entiers premiers entre eux, alors pour tout entier c,
$$a|bc \Rightarrow a|c.$$

Exercice 56
Montrer que le polynôme$P(X) = X^3 - 2$ est irréductible sur $\mathbb{Q}[X]$.

Exercice 57 *Centrale*
Soit $\mathcal{V}$ une partie finie de $\mathbb{C}$ et $I(\mathcal{V})$ l'ensemble des polynômes f de $\mathbb{C}[X]$ tels que $f(x) = 0$ pour tout $x \in \mathcal{V}$.

1. Montrer que $I(\mathcal{V})$ est un idéal de $\mathbb{C}[X]$. Donner un générateur.
2. Soit
$$f(X) = a \prod_{k=1}^{p} (X - \alpha_k)^{\nu_k} \text{ et } \mathcal{V} = \{\alpha_i\}.$$
Montrer que le polynôme $\dfrac{f}{pgcd(f, f')}$, engendre $I(\mathcal{V})$.
3. Déterminer l'idéal $I(\mathcal{V})$ lorsque $\mathcal{V} = f^{-1}(\{0\})$ et $f(X)$ est le polynôme

$$X^{12} + X^{11} + X^{10} + 2\,X^8 + 4\,X^7 + 4\,X^6 + 2\,X^5 + X^4 + 3\,X^3 + 4\,X^2 + 3\,X + 1$$

correction

1. Soient $u \in I = I(\mathcal{V}),\ g \in \mathbb{C}[X]$. On a, pour $a \in \mathcal{V}$, $g.u(a) = g(a)u(a) = 0$ et $g.u \in I$. I est donc un idéal de $\mathbb{C}[X]$.
   Soit $h \in I,\ h(a) = 0$ pour $a \in \mathcal{V}$, et on a, classiquement,

$$\prod_{a\in\mathcal{V}}(X-a) \mid h(X).$$

   Réciproquement, tout multiple de $\prod_{a\in\mathcal{V}}(X-a)$ est dans I.
   On a donc $I =< \phi >,\ \phi = \prod_{a\in\mathcal{V}}(X-a)$.
2. Si $f(X) = a\prod_{k=1}^{p}(X-\alpha_k)^{\nu_k}$, où l'on peut supposer les $\nu_k \neq 0$, on a :

$$Df(X) = a\sum_{j=1}^{p}\left(\left(\prod_{\substack{k=1\\k\neq j}}^{p}(X-\alpha_k)^{\nu_k}\right)\nu_j(X-\alpha_j)^{\nu_j-1}\right)$$

$$\text{pgcd}(f, D(f)) = a\prod_{k=1}^{p}(X-\alpha_k)^{\nu_k-1}$$

$$\phi = \frac{f}{pgcd(f, D(f))} = \prod_{j=1}^{p}(X-\alpha_j).$$

3.
```
F:=X^12+X^11+X^10+2*X^8+4*X^7+4*X^6+2*X^5+X^4+3*X^3+4*X^2+3*X+1;
DF:=diff(F,X);
phi:= quo(F,gcd(F,DF),X);
```
   On obtient $\phi = X^5 + X + 1$.

7 Algorithmique

7.1 Algorithme d'Euclide étendu

• L'algorithme pour les nombres est décrit dans l'exercice 2. Donnons un programme récursif pour la division euclidienne et l'algorithme d'Euclide simple,

```
DivEucl:=proc(a,b)
#=================
local q,r;
if b=0 then Error(cat("dans ", procname, ", division par 0"));
      elif a < b
         then [0,a];
         else DivEucl(a-b,b)+[1,0];
fi;
end:

Euclide:=proc(a,b)
#=================
 if b=0 then a
        else
          DivEucl(a,b);
          Euclide(b,%[2]);
 fi;
 end:
```

puis un un programme itératif avec une boucle while pour l'algorithme d'Euclide étendu aux coefficients de Bezout, on utilise les matrices comme dans l'exercice 2, mais ce n'est pas ce que vous feriez à la main, attention :

```
Bezout:=proc(a,b)
#===============
local r0,r1,q, r, M;
r0:=max(a,b);
r1:=min(a,b);
M:=diag(1,1);

while r1<0 do
  DivEucl(r0,r1);
  q:=%[1];
  r:=%%[2]:
  r0:=r1; r1:=r;
  M:=evalm(matrix([[0,1],[1,-q]])&*M);
od;
r0,M[1,1],M[1,2]
end:
```

• Pour les polynômes nous écrirons

```
DivEuclPoly:=proc(A,B,X)
#======================
    local Q1, Q, R,p,q ;
    option trace;

    p:=degree(A);
    q:=degree(B);
    if p < q
          then [0, A];
          else
             R:=A;
             Q  := 0;
             while (degree(R) = q) do
                     p:= degree(R);
                     Q1:= coeff(R,X,p)/coeff(B,X,q)*X^(p-q);
                     Q := Q + Q1;
                     R:= (sort@expand)(R-Q1*B);
             od;
    fi;
    [Q,R];
    end:
```

7.2 Décomposition d'une permutation en produit de transpositions

Exercice 58 *mise en œuvre de la méthode*
Programmation : on se propose d'implémenter l'algorithme que sous-tend la démonstration du théorème 48. On représentera pour cela les permutations par des listes.

1. Écrire une fonction MAPLE, **Composer2(T,S)** qui prend pour arguments deux listes de $n \geq 2$ entiers (de 1 à n) représentant deux permutations, et retourne la liste représentant le produit de ces deux permutations ;
2. Écrire une fonction MAPLE, **Composer(LL)** qui prend pour argument une liste de listes de $n \geq 2$ éléments, $LL = [L_1, ...L_p]$, et retourne la permutation produit $L_1 \circ ... \circ L_p$.
3. Écrire une fonction MAPLE, **Transp(i,j,n)** qui prend pour arguments trois entiers et retourne la liste de n éléments représentant la transposition $(i,\ j)_n$;
4. Écrire une fonction MAPLE, **DecompTransp(L)** qui prend pour argument une liste L d'entiers, représentant une permutation et retourne une liste de (listes représentant des) transpositions dont le produit est égal à L.
   On écrira une procédure récursive, suivant pas à pas l'algorithme donné par la démonstration du théorème 48. On vérifiera chaque étape au fur et à mesure de son écriture. [4]

4. fichier : Permutations.mws

7.3 Exponentiation rapide et Codage RSA

Exercice 59 *On se propose de mettre en œuvre la méthode de cryptage à clef publique décrite dans l'exercice 50*
On a vu, dans cet exercice que lorsque $n = pq$ est un produit de deux facteurs premiers,
– si d est premier avec $\phi(n) = (p-1)(q-1)$,
– si $\bar{d}\bar{e} = \bar{1}$ dans $\mathbb{Z}/w\mathbb{Z}$ où $w = \phi(n)$,
alors les applications

$$crypt : \bar{m} \in \mathbb{Z}/n\mathbb{Z} \to \bar{m}^e \in \mathbb{Z}/n\mathbb{Z},$$

$$decrypt : \bar{c} \in \mathbb{Z}/n\mathbb{Z} \to \bar{c}^d \in \mathbb{Z}/n\mathbb{Z},$$

sont réciproques l'une de l'autre. Cela fournit une méthode de cryptage à clef publique.
En effet, l'individu A se donne p, q, deux grands nombres premiers, il calcule n, d et e.
Il rend publique la fonction *crypt*, (donc n et e). Il garde secrets p, q et d.
On lui envoie des messages avec *crypt*, il est seul à pouvoir les décrypter tant qu'il reste le seul à savoir factoriser n **en un temps raisonnable.**

1. Que sont les fonctions **mod, isprime, is(a, odd), ifactor, igcd ?** La fonction **isolve** permet elle de résoudre une équation Diophantienne

$$ed + kw = 1?$$

2. Écrire une fonction MAPLE qui prend en argument un nombre entier positif a et retourne le plus petit nombre premier $p \geq a$. Donnez vous p et q premiers de quelques chiffres, puis de plus de 20 chiffres (mesurer le temps de calcul) . Déterminer n et w.
3. La fonction **ifactor** est elle performante ? Utiliser un ordinateur auxiliaire pendant que vous travaillez sur le votre.
4. Regarder ce que l'on peut faire avec la fonction **rand(6)**.
   Écrire une fonction MAPLE qui prend un entier u en argument, détermine un nombre entre 1 et u au hasard, puis retourne le premier entier premier avec u dans $[1, u-1]$.
5. On se donne un nombre d; calculer e. On pourra utiliser l'algorithme d'Euclide étendu donnant des coefficients de Bezout ou la fonction **isolve** de MAPLE.
6. Calculer m^e pour m assez grand. Quel problème rencontrez vous ?
   Pour éviter ce problème utiliser une fonction exponentielle rapide **modulo n :**

```
ExpoRapide:=proc(a,b,n)
 local r;
  if b = 0 then 1;
          elif b = 1 then a mod n
          elif (b  mod 2) = 0 then
                r:=ExpoRapide(a,b/2,n);
                r^2 mod n;
           elif (b mod 2)= 1 then
               r:=ExpoRapide(a,(b-1)/2,n);
               (a*r mod n)*r mod n;
  fi;
  end:
```

```
> ExpoRapide(2,6,5);
                        4
```

7. Écrire des fonctions **Crypt(m,e,n), Decrypt(c,d,n)** comme il se doit.
   Distribuer **Crypt**, garder **DeCrypt**

8 Résumons nous

8.1 Groupes

Définition 13 *rappel du vocabulaire de base*

groupe : Soit E un ensemble non vide et $\star$ une loi interne sur E. On dit que $(E, \star)$ est un groupe ssi
- la loi $\star$ est associative ;
- il existe $e \in E$ tel que $\forall x \in E$, $x \star e = e \star x = x$ (on dit que e est élément neutre pour $\star$)
- pour tout $x \in E$ il existe $x' \in E$ tel que $x \star x' = x' \star x = e$, (on dit que x' est inverse ou symétrique de x).

sous-groupe Soit $(E, \star)$ un groupe d'élément neutre e, on dit qu'une partie H de E est un sous groupe de $(E, \star)$ ssi
- H est non vide ;
- pour tout couple (x, y) d'éléments de H, $x \star y^{-1} \in H$.

ordre d'un groupe on appelle ordre d'un groupe fini, le nombre de ses éléments ;

partie génératrice on dit qu'une partie F d'un groupe G, est une partie génératrice de G', sous-groupe de G ssi G' est le plus petit sous-groupe contenant F;

groupe monogène c'est un groupe engendré par un de ses éléments

groupe cyclique c'est un groupe monogène fini (voir le théorème 35) ;

générateur a est générateur d'un groupe (nécessairement monogène ou cyclique) si $\{a\}$ est une partie génératrice de ce groupe ; l'ordre d'un élément de G est l'ordre du sous-groupe qu'il engendre ;

morphismes une application $f : (G, \star) \to (H, *)$ est un morphisms de groupe ssi pour tous $(a, b) \in G^2$ on a $f(a \star b) = f(a) * f(b)$;

noyau avec les mêmes notations, le noyau d'un morphisms f est le sous groupe de G formé des antécédents de l'unité de H;

isomorphisme c'est un morphisms bijectif ;

Théorème 34 *théorème de Lagrange*[5]
Soit G un groupe fini de cardinal n, H un sous-groupe de G. Alors, l'ordre de H est un diviseur de l'ordre de G.

Théorème 35 *groupes monogènes et cycliques*

1. Soit $(G, *)$, un groupe et $\omega \in G$. Le sous groupe de G engendré par ω est de la forme $\{w^q;\ q \in \mathbb{Z}\}$.
2. Lorsque le groupe monogène engendré par a est infini, les suites $(0, a, 2a, 3a, ...(n-1)a, ...)$ ou $(a^0 = e, a^1, a^2, ..., a^{n-1}e, , ...)$ ont des termes distincts et $G = \{a^q;\ q \in \mathbb{Z}\}$;

5. ce n'est pas au programme, mais je préfère que vous l'ayez vu

3. Tout sous-groupe cyclique d'ordre n, $(G, \star)$ est de la forme $\{\omega^0 = e, \omega^1, ...\omega^{n-1}\}$ et il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.
4. en notation additive, le groupe cyclique engendré par a est de la forme $\{0, a, 2a, 3a, ...(n-1)a\}$ avec $na = 0$;
5. en notation multiplicative, le groupe cyclique engendré par a est de la forme $\{a^0 = e, a^1, a^2, ..., a^{n-1}e\}$, $a^n = e$;

Exemples :
– $(\mathbb{Z}, +)$ est monogène, engendré par ± 1;
– $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe additif cyclique : ses éléments générateurs sont les classes des entiers premiers avec n;
– pour $n \in \mathbb{N}, n > 1$, le groupe des racines $n^{ièmes}$ de l'unité dans $\mathbb{C}$ est un groupe pour la multiplication, cyclique, ses générateurs sont les racines primitives $e^{2ik\pi/n}$ où k est premier avec n;

8.2 Anneaux et corps, généralités, notion d'idéal

Définition 14 *anneaux commutatifs, corps et idéaux*

1. Un ensemble A muni de deux LCI notées $+$ et $\times$ est un **anneau** ssi
   – $(A, +)$ est un groupe commutatif;
   – la loi $\times$ est distributive par rapport à $+$:
     – $(a + b) \times c = a \times c + b \times c,\ c \times (a + b) = c \times a + c \times b$;
     – A possède un élément neutre pour $\times$;
   On dit que A est un **anneau d'intégrité si,** de plus :
   $$xy = 0 \Rightarrow x = 0 \text{ ou } y = 0;$$
2. On dit que l'anneau $(A, +, \times)$ est un **corps** ssi tout élément non nul de A est inversible (pour $\times$) (c'est alors un anneau d'intégrité);
3. Une partie non vide de $I \subset A$, est un **sous-anneau** si c'est un sous-groupe de $(A, +)$ qui est aussi stable pour la loi $\times$ et contient l'élément neutre.
4. Soient $(A, +, \times)$ et $(B, +, \star)$ deux anneaux; on dit qu'une application ϕ de A vers B est un **morphisme d'anneaux** lorsque
   – c'est un morphisme de groupes de $(A, +)$ vers $(B, +)$;
   – on a la formule : $\phi(a \times b) = \phi(a) \star \phi(b)$;
5. **produit de deux anneaux** $(A, +, \times)$ **et** $(B, +, \times)$, c'est l'anneau $(A \times B, +, \times)$ dont les opérations sont définies par
   $$(a, b) + (a', b') = (a + a', b + b') \text{ et } (a, b) \times (a', b') = (aa', bb');$$
6. Dans un anneau d'intégrité commutatif, on définit une relation de **divisibilité** en posant :
   $$a|b \Leftrightarrow \exists d \in A,\ b = da \Leftrightarrow bA \subset aA;$$

On observera sans peine que **l'ensemble des éléments inversibles d'un anneau** $(A, +, \times)$ **forme un groupe multiplicatif (et qui se confond avec** $A\backslash\{0\}$ **ssi** A **est un corps !) ;** par exemple
– le groupe des éléments inversibles de $\mathbb{Z}$ est $\{-1, 1\}$;
– le groupe des éléments inversibles de $\mathbb{K}[X]$ est $\mathbb{K}^*$ (constantes non nulles) ;
– Voir aussi le théorème 46, pour ce qui est des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Définition 15 *idéal*
Soit A un anneau de lois $+$ et $\times$. Un idéal de A est une partie $\mathcal{I}$, de A est un sous-groupe de $(A, +)$ tel que

$$\forall x \in A,\ \ \forall j \in \mathcal{I},\ \ x \times j \in \mathcal{I} \text{ et } j \times x \in \mathcal{I}.$$

8.3 Compléments d'arithmétique, les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$

• Division euclidienne dans l'anneau $\mathbb{Z}$

Théorème 36
Pour tout couple d'entiers naturels (a, b) tel que $b > 0$, il existe un couple (q, r) et un seul vérifiant :

$$a = bq + r \text{ et } 0 \leq r < b.$$

• Division euclidienne dans l'anneau $\mathbb{K}[X]$

Théorème 37
Soit $\mathbb{K}$ un corps. L'anneau des polynômes sur $\mathbb{K}$ est un anneau d'intégrité, et pour tout couple $(A(X), B(X)) \in \mathbb{K}[X] \times (\mathbb{K}[X]/\{0\})$, il existe un unique couple $(Q(X), R(X))$, tel que

$A(X) = Q(X)B(X) + R(X)$ et $degR(X) < deqB(X)$.

• Nombres premiers dans $\mathbb{Z}$

Théorème 38
Tout entier naturel $n > 1$ est d'une façon et d'une seule produit de facteurs premiers :

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$$

où les α_p non nuls sont en nombre fini.

• Polynômes irréductibles dans $\mathbb{K}[X]$

Définition 16
$P \in \mathbb{K}[X]$ *est irréductible dans* $\mathbb{K}[X]$ *ssi*

$$P = QR \Rightarrow P \in \mathbb{K} ou R \in \mathbb{K}.$$

• Idéaux de $\mathbb{Z}$

Théorème 39
1. Les idéaux de $\mathbb{Z}$ sont les parties $a\mathbb{Z}$, $a \in \mathbb{Z}$.
2. $a|b$ ssi $b\mathbb{Z} \subset a\mathbb{Z}$;
3. L'intersection des idéaux $a\mathbb{Z}$ et $b\mathbb{Z}$ est l'idéal $m\mathbb{Z}$ où m est le ppcm de a et de b;
4.Soient a et b deux entiers non nuls, l'idéal engendré par a et b est l'ensemble $\{au + bv;\ (u, v) \in \mathbb{Z}^2\} = d\mathbb{Z}$ où $d = pgcd(a, b)$ est le plus grand diviseur commun de a et de b.

• Idéaux de $\mathbb{K}[X]$

Théorème 40
Dans $\mathbb{K}[X]$, tout idéal $\mathcal{I}$ est formé des multiples d'un polynôme $G(X)$. On dit que G est un générateur de $\mathcal{I}$. Il est unique à une constante multiplicative prés, ie :
$G(X) \times \mathbb{K}[X] = H(X) \times \mathbb{K}[X] \Rightarrow (\exists \alpha \in \mathbb{K},\ G = \alpha H)$.

Notion de polynôme minimal (d'un endomorphisme)

Définition 17
Soit u un endomorphisme de E $\mathbb{K}-ev$. L'ensemble des polynômes annulateurs de u est un idéal de $\mathbb{K}[X]$. On appelle polynôme minimal de u le polynôme générateur de cet idéal dont le coefficient de tête est égal à 1.

• Entiers premiers entre eux

Définition 18
Deux entiers sont premiers entre eux ssi leur pgcd est égal à 1.

Théorème 41 *théorème de Gauss*
Si deux entiers a et b sont premiers entre eux, alors $a|\, b\, x \Rightarrow a|x$.

Théorème 42 *théorème de Bezout*
Soient a et b deux entiers non nuls. Les propositions suivantes sont équivalentes :
1. a et b sont premiers entre eux,
2. l'idéal $\{au + bv;\ (u, v) \in \mathbb{Z}^2\}$ est égal à $\mathbb{Z}$,
3. il existe deux entiers u et v tels que

$$au + bv = 1.$$

• Polynômes premiers entre eux

Définition 19 Deux polynômes A et B sont premiers entre eux ssi leurs seuls diviseurs communs sont les constantes non nulles.

Théorème 43 *théorème de Gauss*
Si A et B sont des polynômes premiers entre eux, alors pour tout polynôme C, $A|BC \Rightarrow A|C$.

Théorème 44 *théorème de Bezout*
Soient A et B deux polynômes. Les propositions suivantes sont équivalentes :
1. A et B sont premiers entre eux,
2. l'idéal $\{AP + BQ;\ (P, Q) \in \mathbb{K}[X]^2\}$ est égal à $\mathbb{K}[X]$,
3. il existe deux polynômes P et Q tels que

$$AP + BQ = 1.$$

Application : la démonstration du lemme des noyaux...

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

Théorème 45 *l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

1. Soit $n \in \mathbb{N}^* \backslash \{1\}$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes des éléments de $\mathbb{Z}$ modulo n. Il y a n classes qui sont celles des entiers 0,1,...,$n-1$.
2. On définit deux lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ en posant :
   - $\bar{a} + \bar{b} = \overline{a+b}$;
   - $\bar{a} \times \bar{b} = \overline{a \times b}$;
3. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition et de la multiplication ainsi définies est un anneau commutatif ;
4. L'application $a \in \mathbb{Z} \to \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ (morphisme canonique) est un morphisme d'anneau surjectif.

Théorème 46 *groupe des inversibles de* $\mathbb{Z}/n\mathbb{Z}$

1. Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ forment un groupe (noté parfois $(\mathbb{Z}/n\mathbb{Z})^\times$) ;
2. un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible ssi il est premier avec n;
3. un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible ssi c'est un élément générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$;
4. $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier ; dans ce cas, le groupe des inversibles est $\mathbb{Z}/n\mathbb{Z}\backslash\{0\}$;

Définition 20 *indicatrice d'Euler*
On appelle indicatrice d'Euler l'application $\phi : \mathbb{N} \to \mathbb{N}$ définie par

$$\phi(n) = Card\left((\mathbb{Z}/n\mathbb{Z})^\times\right).$$

C'est aussi le nombre des entiers $1 \leq p \leq n$, premiers avec n.

Théorème 47 *propriétés de l'indicatrice d'Euler*
– Si p est premier, $\phi(p) = p-1$ et $\phi(p^s) = p^{s-1}(p-1)$;
– si m et n sont premiers entre eux, $\phi(mn) = \phi(m)\phi(n)$;
– pour un naturel n dont la décomposition en facteurs premier est $n = \prod_i p_i^{s_i}$, on a

$$\phi(n) = n\prod_i (1 - 1/p_i).$$

---

9 Quelques corrigés

CO n° 9.1 *corrigé de l'exercice 35.*
Si E est fini (et non vide) pour un élément $z \in E$ quelconque, la suite définie par

$$z_0 = z \text{ et } z_{n+1} = z_n T z_n$$

est aussi finie. L'associativité de T nous permet de noter $z_n = z^{2^n}$ sans perte de sens.

Il existe donc deux entiers $p \in \mathbb{N}$ et $q \geq 1$ tels que $z^{2^{p+q}} = z^{2^p}$. On écrit alors

$z^{2^{p+q}} = z^{2^p}$ puis $z^{2^p} z^{2^p(2^q-1)} = z^{2^{p+q}} = z^{2^p}$ et enfin $z^{2^p} z^{2^p(2^q-2)} z^{2^p(2^q-1)} = z^{2^p} z^{2^p(2^q-2)}$.

L'élément $w = z^{2^p(2^q-1)}$ vérifie donc $wTw = w$.

CO n° 9.2 *corrigé de l'exercice 50. :codage et décodage RSA*

On rappelle que $\phi(n) = n\prod\left(1-\frac{1}{p_i}\right)$.

1. (a) $\phi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 4$ et les éléments inversibles $\bar{x}$, de l'anneau $\mathbb{Z}/12\mathbb{Z}$, sont les classes de $1, 5, 7, 11$.
   Pour chacune de ces classes, on a $\bar{x}^{\phi(n)} = \bar{x}^4 = \bar{1}$; on observe même $\bar{x}^1 = \bar{1}1$
   (b) Qu'en est il dans $\mathbb{Z}/13\mathbb{Z}$?
   $\phi(13) = 12$ (13 est premier) ; les classes de $1, 2, 3, ..., 12$ sont toutes inversibles ($\mathbb{Z}/13\mathbb{Z}$ est un corps) et vérifient $\bar{x}^{\phi(n)} = \bar{x}^{12} = \bar{1}$.
2. Généralisation : Soit $\bar{a}$ un élément inversible de $\mathbb{Z}/n\mathbb{Z}$ et l'application

$$h : \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times \to \bar{a}\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

   (a) h est injective : en effet supposons que $h(x) = \bar{a}x = h(y) = \bar{a}y$. Comme $\bar{a}$ est inversible, en multipliant par $\bar{a}^{-1}$, il vient $x = y$.
   L'ensemble d'arrivée et l'ensemble de départ sont finis et ont le même cardinal, h est donc aussi surjective.
   (b) Calculons $\prod_{\bar{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} h(\bar{x})$, en remplaçant $h(\bar{x})$ par sa définition puis en observant que $h(\bar{x})$ décrit bijectivement $(\mathbb{Z}/n\mathbb{Z})^\times$ lorsque $\bar{x}$ décrit $(\mathbb{Z}/n\mathbb{Z})^\times$:

$$\begin{aligned}\prod_{\bar{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} h(\bar{x}) &= \prod_{\bar{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \bar{a}\bar{x} \\ &= \bar{a}^{\phi(n)} \prod_{\bar{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \bar{x}\end{aligned}$$

$$\prod_{\bar{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} h(\bar{x}) = \prod_{\bar{x}\in(\mathbb{Z}/n\mathbb{Z})^\times} \bar{x}$$

   En identifiant les deux expressions, il vient (théorème d'Euler)

$$\boxed{\bar{a}^{\phi(n)} = \bar{1}.} \tag{9.1}$$

3. p et q sont deux premiers positifs distincts $n = pq$ et $w = \phi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right) = (p-1)(q-1)$.
   (a) Dire qu'il existe $e \in \mathbb{N}$ tel que $\bar{d}\bar{e} = \bar{1}$ dans $\mathbb{Z}/w\mathbb{Z}$ c'est dire que d et w sont premier entre eux.

Supposons avec l'énoncé que d et e sont inverses dans $\mathbb{Z}/w\mathbb{Z}$ et considérons

$$cod : \bar{m} \in \mathbb{Z}/n\mathbb{Z} \to \bar{m}^e \in \mathbb{Z}/n\mathbb{Z},$$

$$dec : \bar{c} \in \mathbb{Z}/n\mathbb{Z} \to \bar{c}^d \in \mathbb{Z}/n\mathbb{Z}.$$

(b) Soit $\bar{m}$ inversible (dans $\mathbb{Z}/n\mathbb{Z}$). $dec \circ cod(\bar{m}) = (\bar{m}^e)^d$.
Comme les classes de d et de e sont inverses dans $\mathbb{Z}/w\mathbb{Z}$ il existe un entier k tel que $d\,e = 1 + kw$ et, dans $\mathbb{Z}/n\mathbb{Z}$,

$$\boxed{(\bar{m}^e)^d = \bar{m}^{e\,d} = \bar{m}^{1+kw} = \bar{m} \times \left(\bar{m}^{\phi(n)}\right)^k = \bar{m}.} \tag{9.2}$$

(c) Si $\bar{m}$ n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$, m et n ne sont pas premiers entre eux et il existe un entier naturel $d \neq 1$ tel que $d|m$ et $d|n = pq$.

$d \neq 1$ ne peut diviser à la fois p et q qui sont premiers entre eux. Alors, deux cas se présentent :

- $d|p$ et d ne divise pas q :

$$n = \prod_{r\in\mathcal{P}} r^{s_r} = p^{s_p} \prod_{r\in\mathcal{P}\setminus\{p,q\}} r^{s_r} = p^{s_p} \times x.$$

- $d|q$ et d ne divise pas p :

$$n = \prod_{r\in\mathcal{P}} r^{s_r} = p^{s_q} \prod_{r\in\mathcal{P}\setminus\{p,q\}} r^{s_r} = q^{s_q} \times x.$$

(d) Considérons m tel que $1 \leq m \leq n-1$ et $m = xp^s$ où x est premier avec n.

$$\begin{aligned} dec \circ cod(\bar{m}) &= ((x\bar{p}^s)^e)^d \\ &= \bar{x}^{ed} \times \bar{p^s}^{ed} \\ &= \bar{x} \times \bar{p^s}^{ed} \\ &= \bar{x} \times \bar{p^s}^{1+k(p-1)(q-1)} \end{aligned}$$

Que vaut $\bar{p}^{ed}$ dans $\mathbb{Z}/n\mathbb{Z}$?
$\bar{p}^{ed} = \bar{p} = 0$ dans $\mathbb{Z}/p\mathbb{Z}$;
$\bar{p}^{ed} = \bar{p}$ dans $\mathbb{Z}/p\mathbb{Z}$ car $\bar{p}^{(p-1)(q-1)} = \left(\bar{p}^{\phi(q)}\right)^{p-1} = \bar{1}$ dans $\mathbb{Z}/q\mathbb{Z}$ par le théorème d'Euler (9.1).
Ainsi $p^{ed} - p$ est il un multiple de p et de q donc de n par le théorème de Gauss et $p^{de} = p$ dans $\mathbb{Z}/n\mathbb{Z}$. En conséquence : $dec \circ cod(\bar{m}) = \bar{x} \times \bar{p^s}^{1+k(p-1)(q-1)} = \bar{x} \times \bar{p^s} = \bar{m}$.

(e) $dec \circ cod$ est l'identité sur $\mathbb{Z}/n\mathbb{Z}$ cqfd.

pour une mise en œuvre, voir le TD MAPLE proposé en section (59) et corrigé sur `mpcezanne.fr` *page MAPLE.*

10 Autres exemples de groupes et de leurs sous-groupes

10.1 Groupe symétrique

10.1.1 Les permutations

Pour tout entier naturel, $n \geq 1$, on note [1,n] l'ensemble des entiers compris entre 1 et n tant qu'il n'y a pas de risque de confusion.

Définition 21 *permutations : vocabulaire et notations*

- Une **permutation** de $[1, n]$ est une bijection de $[1, n]$ dans lui-même ;
- L'ensemble des permutations de $[1, n]$ est noté $\mathcal{S}_n$; muni de la composition des applications, c'est un groupe à $n!$ éléments, que l'on appelle **groupe symétrique ;**
- Le **support** d'une permutation de $[1, n]$ est l'ensemble des éléments $i \in [1, n]$ qui vérifient $\sigma(i) \neq i$;
- On adopte pour une permutation,
  - tantôt une représentation à une ligne : $\sigma = [\sigma_1, \sigma_2, ..., \sigma_n]$, où le terme d'indice i de la liste est $\sigma_i = \sigma(i)$;
  - tantôt une représentation à deux lignes :

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & \dots & n \\ \sigma_1 & \sigma_2 & \sigma_3 & \dots & \sigma_n \end{bmatrix},$$

dans laquelle un terme de la deuxième ligne est l'image du terme de la première ligne situé dans la même colonne. Il est alors possible de ne faire figurer en première ligne que les éléments du support, ainsi :

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{bmatrix},$$

s'écrira aussi

$$\begin{bmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{bmatrix}_5.$$

- Une **transposition** est une permutation dont le support contient deux éléments ; on note $(i, j)_n$ la permutation de $[1, n]$ qui a pour support $\{i, j\}$ (et donc qui échange i et j) ;
- On appelle **k-cycle** une permutation dont le support contient k éléments exactement et telle qu'il existe une numérotation des éléments du support pour laquelle

$$\sigma(a_i) = a_{i+1} \text{ pour } 1 \leq i \leq k-1, \quad \sigma(a_k) = a_1$$

Exercice 60 *pour se faire la main :*

1. Expliciter $(2, 4)_7$.
2. Expliciter les groupes $\mathcal{S}_2$, $\mathcal{S}_3$ et $\mathcal{S}_4$;
3. Expliciter les tables des groupes $\mathcal{S}_2$et $\mathcal{S}_3$;
4. Vérifier que si $\tau = (i, j)_n$ est une transposition, alors $\tau^{-1} = \tau$.
5. Soient $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{bmatrix}$, et $\mu = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{bmatrix}$.
   Calculer σ^{-1}, μ^{-1}, $\sigma \circ \mu$, $\mu \circ \sigma$...

Théorème 48 *théorème fondamental*
Soit n un entier tel que $n \geq 2$. Toute permutation de $\mathcal{S}_n$est un produit de transpositions.

Démonstration par récurrence :
Lorsque $n = 2$, le résultat est évident puisque $\mathcal{S}_2$contient deux éléments, $(1, 2)$ et l'identité ; Supposons le résultat établi pour un entier $n \geq 2$. Considérons alors $\sigma \in \mathcal{S}_{n+1,}$deux cas se présentent :
– soit $\sigma(n+1) = n+1$, et la restriction de σ à [1,n] est un élément de $\mathcal{S}_{n.}$On a donc

$$\sigma_{|[1,n]} = \prod (i_k, j_k)_n \text{ et } \sigma = \prod (i_k, j_k)_{n+1};$$

– soit $\sigma(n+1) \neq n+1$, et on se ramène au cas précédent en considérant le produit

$$\tau \circ \sigma = (\sigma(n+1),\, n+1)_{n+1} \circ \sigma$$

qui est un élément de $\mathcal{S}_{n+1}$ laissant $n+1$ invariant.
□

Exercice 61 *mise en œuvre de la méthode*

1. Décomposer la permutation suivante en produit de transpositions en suivant la méthode décrite par la démonstration précédente :

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{bmatrix}.$$

2. Programmation : voir l'exercice 58.

10.1.2 Signature d'une permutation

Théorème 49 Si une permutation de $\mathcal{S}_n$(avec $n \geq 2$), s'écrit

$$\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_p = \mu_1 \circ \mu_2 \circ ... \circ \mu_q,$$

où les τ_i, μ_j sont des transpositions, alors les entiers p et q ont la même parité.

Démonstration : HP

Définition 22 Soit $\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_p \in \mathcal{S}_n$, comme ci-dessus. Le nombre $(-1)^p$ ne dépend que de σ. On l'appelle signature de σ, on le note $\varepsilon(\sigma)$.

Théorème 50
L'application $\varepsilon : (\mathcal{S}_n, \circ) \to (\{-1, 1\}, \times)$ est un homomorphisme de groupes.

Démonstration : facile.

10.1.3 Exercices

Exercice 62 *cycles*
Soient i, j, n tels que $1 \leq i < j \leq n$.

1. Exprimer plus simplement $(1,i)_n \circ (1,j)_n \circ (1,i)_n$.
2. Exprimer plus simplement $(1,n)_n \circ (1,n-1)_n \circ ... \circ (1,3)_n \circ (1,2)_n$.
3. Montrer que tout cycle $(c_1 \to c_2 \to ... \to c_k \to c_1)_n$ se décompose en produit de transpositions de la forme $(1,j)_n$.
4. Soit c un $k-$cycle de $\mathcal{S}_n$.Quelle est sa signature ?

Exercice 63 Soit E un ev de dimension n, de base $\mathcal{B}$. A toute permutation de $\mathcal{S}_n$, on associe l'endomorphisme f_σ de E défini par :

$$\forall i, f_\sigma(b_i) = b_{\sigma(b_i)}.$$

On notera M_σ la matrice dans la base $\mathcal{B}$.

1. Expliciter ces matrices lorsque $n = 3$;
2. Déterminer M_σ^{-1}
3. Vérifier que
$$\sigma \in (S_n, \circ) \to f_\sigma \in \mathcal{GL}(E)$$
est un morphisme de groupe.

10.2 Le groupe orthogonal

10.2.1 Généralités

Théorème 51 *groupe orthogonal*

– L'ensemble des endomorphismes orthogonaux de E euclidien forme un groupe pour la compositions des endomorphismes. On le note $(O(E), \circ)$
– L'ensemble des endomorphismes orthogonaux tels que $Det(u) = +1$ est un sous-groupe de $O(E)$ noté $O^+(E)$. Ce sous groupe est commutatif ssi $dimE \leq 2$;
– L'ensemble des matrices orthogonales de $\mathcal{M}_n(\mathbb{R})$ forme un groupe pour la multiplication des matrices. On le note $(O_n(\mathbb{R}), \times)$.
– L'ensemble des matrices orthogonales telles que $Det(M) = +1$ est un sous-groupe de $O_n(\mathbb{R})$ noté $O_n^+(\mathbb{R})$.

Définition 23 *symétries orthogonales et réflexions*
On appelle symétrie orthogonale une symétrie dont les sous-espaces propres $ker(f - id)$ et $ker(f + id)$ sont supplémentaires orthogonaux.
Une réflexion est une symétrie orthogonale par rapport à un hyperplan.

10.2.2 Description de $O_2(\mathbb{R})$ et de $O_3(\mathbb{R})$

Nous donnons ici de brefs rappels du cours de première année. On note dans les tableaux qui suivent $E_1 = ker(u - id_E) = \{x;\ u(x) = x\}$ et $E_{-1} = ker(u + id_E) = \{x;\ u(x) = -x\}$.

En dimension 2 nous avons :

Det	Spectre	Éléments propres	Nature géométrique	Matrice (BON)
1	$\{1\}$	$E_1 = E$	id_E	I_2
1	$\{-1\}$	$E_{-1} = E$	$-id_E$, rotation d'angle π	$-I_2$
1	vide	...	rotation d'angle $\theta \neq 0[\pi]$	$\begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}$
-1	$\{1,-1\}$	$D = E_1, \perp D = E_{-1}$	réflexion d'axe D tq $(\widehat{Ox, D}) = \theta/2$	$\begin{bmatrix}\cos(\theta) & \sin(\theta)\\ \sin(\theta) & -\cos(\theta)\end{bmatrix}$

• La matrice d'une rotation est inchangée par changement de BON **directe** le paramètre θ change de signe avec un changement de BON indirecte.
• La matrice d'une réflexion change avec la BON, le paramètre θ est le demi-angle entre e_1 et l'axe de la réflexion ;
• $O_2^+(\mathbb{R})$ est commutatif (cela devient faux si $n \geq 3$).

En dimension 3, le polynôme caractéristique est de degré impair, le spectre contient un des réels 1 ou -1 au moins et nous avons :

Det	Spectre	Éléments propres	Nature géométrique
1	$\{1\}$	$E_1 = E$	id_E
1	$\{1\}$	$dim E_1 = 1$	rotation d'axe E_1
-1	$\{-1\}$	$dim E_{-1} = 3$	symétrie centrale, produit de 3 réflexions
-1	$\{-1,1\}$	$dim E_1 = 2$	réflexion de plan E_1
-1	$\{-1\}$	$dim E_{-1} = 1$	produit d'une rotation et d'une réflexion (avec $D \perp P$)

Théorème 52 Soit $u \in O(E)$, un endomorphisme orthogonal.
• si $dim E = 2$, u est une réflexion ou composé de 2 réflexions ;
• si $dim E = 3$, u est une réflexion ou composé de 2 ou 3 réflexions ;
Dans les deux cas, les **réflexions engendrent le groupe orthogonal.**

Index