Algèbre M1 MIC

Notes de cours

Auteur
Thomas Arrous

12 septembre 2024

Table des matières

1 Introduction

Ce document est un recueil de notes de cours d'algèbre niveau M1. Il est basé sur un cours de l'Université Paris Cité, cependant toute erreur ou inexactitude est de ma responsabilité.

Toute erreur signalée ou remarque est la bienvenue. Sentez-vous libres de contribuer à ce document par le biais de GitHub.

2 Division euclidienne

Theorem 1 (Division euclidienne)**.** *$\forall$ a $\in \mathbb{Z}$, $\forall$ b $\geq$ 1, $\exists$! (q,r) $\in \mathbb{Z}^2$ tel que :*

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \quad \textit{avec } q = \textit{quotient et } r = \textit{reste.}$$

On dit que : $\begin{cases} b \textit{ divise } a \\ a \textit{ est un multiple de } b \end{cases}$ *si $\exists$ k tel que $a = bk$ on note $b|a$.*
C'est une relation d'ordre sur $\mathbb{N}$ = {0, 1 ,2 , ...}
Plus grand élément : 0
Plus petit élément : 1

Rappel 1 (relation d'ordre)**.** *Dans un ensemble E, on appelle relation d'ordre, notée ici R à la fois :*

$$\begin{cases} \textit{réflexive : pour tout x de E, x R x} \\ \textit{antisymétrique : pour tous les x et y de E tels que x R y et y R x, alors x = y} \\ \textit{transitive : pour tous les x, y et z de E tels que x R y et y R z, alors x R z} \end{cases}$$

Définition 1 (pgcd/ppcm)**.** *Soit $a_1, a_2, ..., a_k \in \mathbb{Z}$ leur pgcd, noté $a_1 \wedge ... \wedge a_k$ est le plus grand diviseur commun à a_1 , ..., a_k dans $\mathbb{N}$ pour la relation.*

Exemple 1. *exemple :* $0 \wedge a = a$

Définition 2. *le ppcm est définit de façon analogue ppcm $(a_1, ..., a_k) = a_1 \vee ... \vee a_k$.*

Proposition 1 (Identité de Bézout)**.** *$\forall$ a,b $\in \mathbb{Z}$, $d = a \wedge b$, $\exists$ (u,v) $\in \mathbb{Z}$ tel que au + bv = d*

Démonstration 1. *preuve algo d'Euclide étendu.*

Exemple 2 (Algo d'euclide étendu)**.** *368 $\wedge$ 117 = ?*

étapes	*1*	*2*	*3*	*4*	*5*	*6*
(r, u, v)	*(368, 1, 0)*	*(117, 0, 1)*	*(17, 1, -3)*	*(15, -6, 19)*	*(2, 7, -22)*	*(1, -55, 173)*
(r', u', v')	*(117, 0, 1)*	*(17, 1, -3)*	*(15, -6, 19)*	*(2, 7, -22)*	*(1, -55, 173)*	*(0, *, *)*
r - αr' = new r	*368 - 3×117 = 17*	*117 - 6×17 = 15*	*17 - 15 = 2*	*15 - 7×2 = 1*	*2 - 2×1 = 0*	

On a : 368×(-55) + 117×173 =1
Donc : 368 $\wedge$ 117 = 1

Définition 3. *Soit a,b $\in \mathbb{Z}$ On dit que a et b sont premier entre eux si $a \wedge b = 1$.*

Définition 4. *Soit n $\in \mathbb{N}^*$ = {1,2,...} On appelle indicatrice d'Euler de n, et on notre $\phi(n)$ le nombre d'éléments de {1,...,n} premier avec n.*

Exemple 3. *$\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$.*

Définition 5. *Un nombre n est premier s'il admet exactement deux diviseur positifs*

Exemple 4. *2,3,5,7,11 ...*

Theorem 2 (Bézout)**.** *$\forall$ a,b $\in \mathbb{Z}$ si $\exists$ u,v $\in \mathbb{Z}$ tq au + bv = 1 alors $a \wedge b = 1$*

Démonstration 2. *Soit d un diviseur commun à a et b.*
d/a, d/b => d/au+bv = 1 => d = 1

Lemme 1 (Lemme d'Euclide)**.** *Soit a, b $\in \mathbb{Z}$ et p premier.*
Si p/ab alors p/a ou p/b

Corollaire 1. *Soit a $\in \mathbb{Z}$, p premier. Alors, soit p divise a, soit $p \wedge a = 1$.*

Corollaire 2. *Si p est premier, alors $\phi(p)$ = p-1.*
n est premier <=> $\phi(n)$ = n-1.

Lemme 2 (Lemme de Gauss)**.** *Soit a,b,c $\in \mathbb{Z}$.*

$$Si \begin{cases} a/bc \\ a \wedge b \end{cases} alors\ a/c$$

Corollaire 3. *Tout nombre $n \in \mathbb{N}$ s'écrit sous la forme $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ où p_i premier 2 à 2 différents, $\alpha_i \geq 1$ unique à permutation près.*

Corollaire 4. *Si p premier et $\alpha \geq 1$*
$\phi(p^\alpha) = p^{\alpha-1}$ (p-1)
$= p^\alpha$ - $p^{\alpha-1}$

Démonstration 3. *Parmi {1, ... p^α}*
si $a \wedge p^\alpha \neq 1$ => $\exists$ $0 < \beta \leq \alpha$, $p^\alpha \wedge a = p^\beta$
=> Les nombres qui ne sont pas premier avec p^α sont les multiples de p.
{p,2p,3p,...$p^{\alpha-1}p$}
Il y en a $p^{\alpha-1}$ donc :
ϕ (p^α) = p^α - $p^{\alpha-1}$ = $p^{\alpha-1}$(p-1)

Theorem 3 (petit théorème de Fermat)**.** *Si p est premier et a $\in \mathbb{Z}$ alors $a^p \equiv a$ [p]*

Lemme 3. *Soit p premier et $1 \leq n \leq$ p-1 un entier alors p divise $\binom{p}{n}$*

Démonstration 4. $\binom{p}{n} = \frac{p!}{n!(p-n)!} = p\frac{(p-1)!}{n!(p-n)!}$
n<p, p-n<p.

Démonstration 5. *Preuve par récurrence du théorème de Fermat :*
$0^p = 0 \equiv$ *0 [p]*
Supposons que : $a^p \equiv a[p]$
$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$
$= a^p + 1^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k$ (HR)
$\equiv$ a+1[p]

Corollaire 5. *Soit p premier et* $a \in \mathbb{Z}$ *premier avec p.*
Alors $a^{p-1} \equiv 1[p]$

Démonstration 6. $a^p \equiv a[p]$ *=> p /* a^p *-a = a(* a^{p-1} *-1)*
lemme de Gauss => p / $a^{p-1} - 1$ *=>* $a^{p-1} \equiv$ *1[p]*

$(\mathbb{Z}/n\mathbb{Z})^\times$ *= {[a]* $\in \mathbb{Z}/n\mathbb{Z}$ *tel que* $\exists$ *[b]* $\in \mathbb{Z}/n\mathbb{Z}$ *tel que [ab] = [1]}*

Exemple 5. $(\mathbb{Z}/2\mathbb{Z})^\times$ *= {[1]}*
$(\mathbb{Z}/3\mathbb{Z})^\times$ *= {[1],[2]}*
$(\mathbb{Z}/4\mathbb{Z})^\times$ *= {[1],[3]}*

Proposition 2. $(\mathbb{Z}/n\mathbb{Z})^\times$ *forme un groupe abélien pour la multiplication.*

Proposition 3. *|*$(\mathbb{Z}/n\mathbb{Z})^\times$*| =* $\phi(n)$

Lemme 4. *Soit a, n* $\in \mathbb{Z}$*, [a]* $\in \mathbb{Z}/n\mathbb{Z}$ *est inversible <=> a* $\wedge$ *n = 1*

Démonstration 7. *Si a est inversible mod n =>* $\exists$ *b* $\in \mathbb{Z}$ *tq ab* $\equiv$ *1[n]*
=> $\exists$ *k* $\in \mathbb{Z}$ */ ab - 1 = kn*
<=> ab - kn =1
=> a$\wedge$*n = 1*
Si a$\wedge$*n = 1, alors* $\exists$ *u,v tq au+nv = 1*
<=> au -1 = -nv
=> au $\equiv$ *1[n]*

Proposition 4. *Soit* $a \in \mathbb{Z}/n\mathbb{Z}$*.*
Alors $a \wedge n = 1$ *<=> a engendre le groupe* $(\mathbb{Z}/n\mathbb{Z}, +)$

Démonstration 8. *Si a*$\wedge$*n =1*
alors $\exists$ *b tq ab =* $\sum_{i=1}^{b} a$ *= a+a+ ... +a (b fois)* $\equiv$ *1[n]*
=> 1 $\in$ *<a> (sous groupe engendré par a)*
=> <a> = $\mathbb{Z}/n\mathbb{Z}$
Si <a> = $\mathbb{Z}/n\mathbb{Z}$
=> 1$\in$*<a>*
=> $\exists$ *b / a+a+ ... +a (b fois) =* $\sum_{i=1}^{b} a$ *= ab* $\equiv$ *1[n]*

Corollaire 6. *Soit* $a \in \mathbb{Z}/n\mathbb{Z}$
$a^{\phi(n)} \equiv 1[n]$

Démonstration 9. *Preuve d'après le thm de Lagrange, l'ordre d de a divise* ϕ*(n)*
=> $(a^d)^? = 1^? = 1 = \phi(n)$

Remarque 1. *Si n est premier* ϕ*(n) = n-1 =>* $a^{n-1} \equiv$ *1 [n]*

Corollaire 7. *(*$\mathbb{Z}/n\mathbb{Z}$*, +,* $\times$*) est un corps <=> n est premier.*

Démonstration 10. $\mathbb{Z}/n\mathbb{Z}$ *est un corps*
<=> $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \backslash \{0\}$
<=> $\phi(n)$ *= n-1*
<=> n est premier

Proposition 5. *Soit p premier, le groupe* $(\mathbb{Z}/p\mathbb{Z})^{\times}$ *est cyclique (d'ordre p-1)*

Lemme 5. *Soit* $n \geq 1$*, alors* $n = \sum_{d|n \ et \ d\geq 0} \phi(d)$

Démonstration 11. *Soit* ν_d *le nombre d'éléments de* $\mathbb{Z}/n\mathbb{Z}$ *d'ordre d.*
On a :
$n = \sum_{d|n} \nu_d$
$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \{a \in \mathbb{Z}/n\mathbb{Z} \ / \ a \text{ est d'ordre } d\}$
Or, $\mathbb{Z}/n\mathbb{Z}$ *ne contient qu'un seul sous groupe d'ordre d, à savoir* $\frac{n}{d} \times \mathbb{Z}/n\mathbb{Z}$
=> ν_d = *nombre de générateur de* $\frac{n}{d} \times \mathbb{Z}/n\mathbb{Z}$

Exemple 6. $n = 36$, $d = 4$
$9\mathbb{Z}/36\mathbb{Z} = \{ 0,9,18,29 \}$
d'après la prop de tout à l'heure, on obtient que : $\nu_d = \phi(d)$

Exemple 7. $\mathbb{Z}/6\mathbb{Z}$

ordre	1	2	3	6
	0	3	2 ; 4	1 ; 5
sous groupe engendré	{0}	{0 ; 3}	{0 ; 2 ; 4}	{0 ; 1 ; 2 ; 3 ; 4 ; 5}

Proposition 6. *Soit* $\mathbb{K}$ *un corps fini. Alors* $\mathbb{K}^{\times}$ *est cyclique*

Démonstration 12. *Soit* ν_d = *nombre d'éléments d'ordre d dans* $K^{\times}$.
Soit $n = |K^{\times}|$
Soit $x \in K^{\times}$ *d'ordre d.*
Alors <x> contient d éléments = $\{1, x, x^2, ..., x^{d-1}\}$
$\forall \ y \in$ <x>, $y^d = 1$
=> *y est racine du polynôme* $Y^d - 1 \in \mathbb{K}[Y]$
Comme $\mathbb{K}$ *est un corps, ce polynôme admet un nombre* $\leq$ *d racines.*
=> *les racines de* y^d *-1 sont exactement les éléments de <x> =* $\mathbb{Z}/d\mathbb{Z}$.
=> *tous les éléments d'ordre d de* $\mathbb{K}^{\times}$ *sont dans <x>*
=> *il contient* ϕ *(d) éléments d'ordre d*
Conclusion :
Soit $\nu_d = 0$
soit $\nu_d = \phi(d)$
=> $\nu_d <= \phi(d) \ \forall \ d$
$n = \sum_{d|n} \nu_d = \sum_{d|n} \phi(d)$
=> *On doit avoir* $\nu_d = \phi(d) \ \forall \ d$ *(sinon la somme de gauche serait < à la somme de droite).*
En particulier , $\nu_n = \phi(n) \neq 0$
=> $K^{\times}$ *contient au moins un élément d'ordre n*
=> $K^{\times}$ *est cyclique.*
$(\mathbb{Z}/p\mathbb{Z})^{\times}$ *est cyclique*
$\exists \ a \in \mathbb{Z}$ *tq* $\mathbb{Z}/p\mathbb{Z} = 1, a, a^2, ..., a^{p-1}$
$a^k = b[p]$

Proposition 7. *Soit p un nombre premier impair et* $\alpha \geq 2$ *un entier.*
Alors $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$ *est cyclique (d'ordre* $\phi(p^{\alpha}) = p^{\alpha-1}(p-1)$*)*
Il suffit de trouver un élément d'ordre $p^{\alpha}(p-1)$

Remarque 2. $p^{\alpha-1} \wedge (p-1) = 1$

Proposition 8. *Soit G un groupe, a un élément d'ordre k, b un élément d'ordre l. Si a et b commutent et si $k \wedge l = 1$, alors ab est d'ordre kl.*
/!\ $k \wedge l \neq 1$, ab n'est pas forcément d'ordre kvl.
$a \times a^{-1} = 1$
/!\ Si a et b ne commutent pas, c'est faux.
Dans S_3 (1 2) (1 2 3)
(1 2) (1 2 3) = (2 3)
=> il suffit de trouver un élément d'ordre p-1 et un autre d'ordre $p^{\alpha-1}$

Lemme 6. *Soit $k \in \mathbb{N}$, $\exists\ \lambda_k \in \mathbb{N}$ premier avec p tel que $(1+p)^{p^k}$ = 1 + $\lambda_k p^{k+1}$*

Démonstration 13. *k = 0*
$(1+p)^{p^0} = (1+p)^1 = 1+p$
$= 1 + \lambda_0 p^{0+1}$ *avec* $(\lambda_0 = 1)$

Supposons le résultat au rang k vrai.
$(1+p)^{p^{k+1}} = ((1+p)^{p^{k+}})^p$
$= (1 + \lambda_k p^{k+1})^p$
$= \sum_{i=0}^{p} (iparmisp) \lambda_k^i p^{(k+1)i}$
$= 1 + \lambda_k p^{k+2} + p^{k+3} u$ *avec* $u \in \mathbb{Z}$
$(1+p)^{p^{k+1}} = 1 + (\lambda_k + up)p^{k+2}$ *avec* $(\lambda_k + up) = \lambda_{k+1}$

Corollaire 8. *1+p $\in \mathbb{Z}/p^\alpha\mathbb{Z}$ est d'ordre $p^{\alpha-1}$*

Démonstration 14. $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1}\ p^\alpha \equiv 1[p^\alpha]$
=> l'ordre de 1+p divise $p^{\alpha-1}$
$(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1}$
Si on avait 1 + $\lambda_{\alpha-2} p^{\alpha-1} \equiv 1[p^\alpha]$
=> $p^\alpha | \lambda_{\alpha-2} p^{\alpha-1}$
=> $p | \lambda_{\alpha-2} impossible$
=> $(1+p)^{p^{\alpha-2}} \not\equiv 1[p^\alpha]$

Proposition 9. *Il existe un élément d'ordre p-1 dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$*

Démonstration 15. *Soit* $\begin{array}{cccc} \psi & : & \mathbb{Z}/p^\alpha\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & & [n] & \mapsto & [n] \end{array}$
=> induit $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ morphisme de groupe.
$(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément x d'ordre p-1.
ψ est surjectif => $\exists$ y $\in$ $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tel que ψ(y) = x.
=> l'ordre de y est un multiple de p-1.
Si d = l'ordre de y
$y^d = 1 => \psi(y^d) = \psi(1) = 1$
et $\psi(y^d) = \psi(y)^d = x^d$
=> p-1/d
(TODO)

Proposition 10. $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ *est isomorphe à :*
$$\begin{cases} \{1\} \text{ si } \alpha = 1 \\ \mathbb{Z}/2\mathbb{Z} \text{ si } \alpha = 2 \\ \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ si } \alpha \geq 3 \end{cases}$$

Exemple 8. $\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z}$
$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$
$3^2 = 9 \equiv 1[8]$
$5^2 = 25 = 1[8]$
$7^2 \equiv 1[8]$

Lemme 7. *Soit* $k \in \mathbb{N}$,
$\exists\ \mu_k$ *impair tel que* $5^{2^k} = 1 + 2^{k+2}\mu_k$

Démonstration 16. *Démonstation de la proposition. Les deux premiers cas sont évidents. Supposons* $\alpha \geq 3$.
$\psi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$
$\psi(2^\alpha) = 2^{\alpha-1}$
ψ(3) = 3
=> 3 est d'ordre pair. Ordre (3) = 2d.

3^d *est d'ordre 2.*
$S : (\mathbb{Z}/4\mathbb{Z})^\times -> (\mathbb{Z}/2^{\alpha-1}Z)^\times[1]|-> [1][3]|-> [3^d]$
$S \circ \phi = id$
$f : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times -> ker(\phi)x(\mathbb{Z}/4\mathbb{Z})^\times[n]|-> [ns(n)^{-1}, \phi(n)]$
Ordre à gauche = ordre à droite = $\phi(2^\alpha) = 2^{\alpha-1}$
|Ker (ψ)| = $\frac{|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times|}{|(\mathbb{Z}/4\mathbb{Z})^\times|} = 2^{\alpha-2}$
5 ∈ ker ψ et 5 est d'ordre $2^{\alpha-2}$
=> 5 engendre ker(ϕ)
$(ker(\phi)) \times (\mathbb{Z}/4\mathbb{Z})^\times$ *est engendré par la famille {(5,1), (1,3)}*
(5, 1) = f(5)
(1, 3) = f(3)
=> f est surjectif.
Comme les deux groupes ont le même ordre, f est une bijection => c'est un iso.
$5^{2^{\alpha-2}} = 1 + \mu_{\alpha-3}2^\alpha$
$\equiv 1[2^\alpha]$
=> l'ordre de 5 divise $2^{\alpha-2}$
$5^{2^k} = 1 + \mu_{\alpha-3}2^{k+2}$, *avec* $k < \alpha - 2$
Si c'était $\equiv 1[2^\alpha]$
$=>2^\alpha|(2^{k+2}\mu_k + 1 - 1)$
$=>2|2^{\alpha-k-2}|\mu_k$

Theorem 4. *des restes chinois*
Soit a,b >= 2 premiers entre eux alors on a un isomorphisme d'anneau.
$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$

Corollaire 9. *Soit* $n \in \mathbb{N}*$
Si $n = 2^{\alpha} p_1^{\alpha_1} p_k^{\alpha_k}$
où $\alpha, \alpha_i >= 0$ *et* $p_1, ..., p_k$ *sont premiers, différents deux à deux, alors :*
$(\mathbb{Z}/n\mathbb{Z})^{\times} \cong$
$(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times} \times (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^{\times} \times ... \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^{\times}$

Theorem 5. *Soit :* $\begin{array}{cccc} f & : & \mathbb{Z}/ab\mathbb{Z} & \rightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & & [n] & \mapsto & ([n],[n]) \end{array}$

Si $n \in$ *ker(f), n≡0[a]*
n≡0[b]
a/n et b/n
=> le ppcm (a,b) = ab divise n.
=> n ≡ 0 [ab]
=> [n] = 0
Si $n = p_1^{\alpha_1}...p_k^{\alpha_k}$
$\phi(n) = \phi(p_1^{\alpha_1})...\phi(p_k^{\alpha_k})$
$= p_1^{\alpha_1 - 1}(p_1 - 1)...p_k^{\alpha_k - 1}(p_k - 1)$
$= n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_k})$

Proposition 11. *Si* $a \wedge b = 1$ *alors* $\phi(ab) = \phi(a)\phi(b)$