
Algèbre M1 MIC

Notes de cours

Auteur
Thomas Arrous

12 septembre 2024

Table des matières

1 Introduction	2
2 Division euclidienne	2

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 :

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

On dit que : $\begin{cases} b \text{ divise } a \\ a \text{ est un multiple de } b \end{cases}$ si $\exists k$ tel que $a = bk$ on note $b|a$.

C'est une relation d'ordre sur $\mathbb{N} = \{0, 1, 2, \dots\}$

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 :

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

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

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

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

Proposition 1 (Identité de Bézout). $\forall a, b \in \mathbb{Z}, d = a \wedge b, \exists (u, v) \in \mathbb{Z}^2$ 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
(r, u, v)	$(368, 1, 0)$	$(117, 0, 1)$	$(17, 1, -3)$	$(15, -6, 19)$
(r', u', v')	$(117, 0, 1)$	$(17, 1, -3)$	$(15, -6, 19)$	$(2, 7, -22)$
$r - \alpha r' = \text{new } r$	$368 - 3 \times 117 = 17$	$117 - 6 \times 17 = 15$	$17 - 15 = 2$	$15 - 7 \times 2 = 1$

On a : $368 \times (-55) + 117 \times 173 = 1$

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 $n \in \mathbb{N}^* = \{1, 2, \dots\}$ On appelle indicatrice d'Euler de n , et on note $\phi(n)$ le nombre d'éléments de $\{1, \dots, n\}$ 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 diviseurs 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 .
 $d|a, d|b \Rightarrow d|au + bv = 1 \Rightarrow d = 1$

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 $\Leftrightarrow \phi(n) = n-1$.

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

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

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

Corollaire 4. Si p premier et $\alpha \geq 1$

$$\begin{aligned} \phi(p^\alpha) &= p^{\alpha-1} (p-1) \\ &= p^\alpha - p^{\alpha-1} \end{aligned}$$

Démonstration 3. Parmi $\{1, \dots, p^\alpha\}$

si $a \wedge p^\alpha \neq 1 \Rightarrow \exists \theta < \beta \leq \alpha, p^\alpha \wedge a = p^\beta$

\Rightarrow Les nombres qui ne sont pas premiers avec p^α sont les multiples de p .

$\{p, 2p, 3p, \dots, p^{\alpha-1}p\}$

Il y en a $p^{\alpha-1}$ donc :

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

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

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 :
 $0^p = 0 \equiv 0 \pmod{p}$

Supposons que : $a^p \equiv a \pmod{p}$

$$\begin{aligned} (a+1)^p &= \sum_{k=0}^p \binom{p}{k} a^k \\ &= a^p + 1^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k \quad (HR) \\ &\equiv a+1 \pmod{p} \end{aligned}$$

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

Démonstration 6. $a^p \equiv a \pmod{p} \Rightarrow p \mid a^p - a = a(a^{p-1} - 1)$
 lemme de Gauss $\Rightarrow p \mid a^{p-1} - 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

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

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 $\Leftrightarrow a \wedge n = 1$

Démonstration 7. Si a est inversible mod $n \Rightarrow \exists b \in \mathbb{Z}$ tq $ab \equiv 1 \pmod{n}$

$$\Rightarrow \exists k \in \mathbb{Z} \mid ab - 1 = kn$$

$$\Leftrightarrow ab - kn = 1$$

$$\Rightarrow a \wedge n = 1$$

Si $a \wedge n = 1$, alors $\exists u, v$ tq $au + nv = 1$

$$\Leftrightarrow au - 1 = -nv$$

$$\Rightarrow au \equiv 1 \pmod{n}$$

Proposition 4. Soit $a \in \mathbb{Z}/n\mathbb{Z}$.

Alors $a \wedge n = 1 \Leftrightarrow a$ engendre le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Démonstration 8. Si $a \wedge n = 1$

alors $\exists b$ tq $ab = \sum_{i=1}^b a = a+a+ \dots +a$ (b fois) $\equiv 1[n]$

$\Rightarrow 1 \in \langle a \rangle$ (sous groupe engendré par a)

$\Rightarrow \langle a \rangle = \mathbb{Z}/n\mathbb{Z}$

Si $\langle a \rangle = \mathbb{Z}/n\mathbb{Z}$

$\Rightarrow 1 \in \langle a \rangle$

$\Rightarrow \exists b \mid a+a+ \dots +a$ (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 $\phi(n)$

$\Rightarrow (a^d)^? = 1^? = 1 = \phi(n)$

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

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

Démonstration 10. $\mathbb{Z}/n\mathbb{Z}$ est un corps

$\Leftrightarrow (\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$

$\Leftrightarrow \phi(n) = n-1$

$\Leftrightarrow n$ 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 $n = \sum_{d \mid n} \text{et } d \geq 0 \phi(d)$

Démonstration 11. Soit ν_d le nombre d'éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d .

On a :

$$n = \sum_{d \mid n} \nu_d$$

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d \mid n} \{a \in \mathbb{Z}/n\mathbb{Z} \mid a \text{ est d'ordre } d\}$$

Or, $\mathbb{Z}/n\mathbb{Z}$ ne contient qu'un seul sous groupe d'ordre d , à savoir $\frac{n}{d} \times \mathbb{Z}/n\mathbb{Z}$

$\Rightarrow \nu_d =$ nombre de générateur de $\frac{n}{d} \times \mathbb{Z}/n\mathbb{Z}$

Exemple 6. $n = 36, d = 4$

$$9\mathbb{Z}/36\mathbb{Z} = \{0, 9, 18, 27\}$$

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 \mathbb{K}^\times .

Soit $n = |\mathbb{K}^\times|$

Soit $x \in \mathbb{K}^\times$ d'ordre d .

Alors $\langle x \rangle$ contient d éléments $= \{1, x, x^2, \dots, x^{d-1}\}$

$\forall y \in \langle x \rangle, y^d = 1$

$\Rightarrow y$ 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.

\Rightarrow les racines de $y^d - 1$ sont exactement les éléments de $\langle x \rangle = \mathbb{Z}/d\mathbb{Z}$.

\Rightarrow tous les éléments d'ordre d de \mathbb{K}^\times sont dans $\langle x \rangle$

\Rightarrow il contient $\phi(d)$ éléments d'ordre d

Conclusion :

Soit $\nu_d = 0$

soit $\nu_d = \phi(d)$

$\Rightarrow \nu_d \leq \phi(d) \forall d$

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

\Rightarrow On doit avoir $\nu_d = \phi(d) \forall d$ (sinon la somme de gauche serait $<$ à la somme de droite).

En particulier, $\nu_n = \phi(n) \neq 0$

$\Rightarrow \mathbb{K}^\times$ contient au moins un élément d'ordre n

$\Rightarrow \mathbb{K}^\times$ est cyclique.

$(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique

$\exists a \in \mathbb{Z} \text{ tq } \mathbb{Z}/p\mathbb{Z} = 1, a, a^2, \dots, a^{p-1}$

$a^k = b[p]$

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 kl .

$a \times a^{-1} = 1$

/!\ Si a et b ne commutent pas, c'est faux.

Dans S_3 $(1 \ 2) (1 \ 2 \ 3)$

$(1 \ 2) (1 \ 2 \ 3) = (2 \ 3)$

\Rightarrow 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. $k = 0$

$$(1+p)^{p^0} = (1+p)^1 = 1+p \\ = 1 + \lambda_0 p^{0+1} \text{ avec } (\lambda_0 = 1)$$

Supposons le résultat au rang k vrai.

$$(1+p)^{p^{k+1}} = ((1+p)^{p^k})^p \\ = (1 + \lambda_k p^{k+1})^p \\ = \sum_{i=0}^p \binom{p}{i} (\lambda_k p^{k+1})^i p^{(k+1)i} \\ = 1 + \lambda_k p^{k+2} + p^{k+3} u \text{ avec } u \in \mathbb{Z} \\ (1+p)^{p^{k+1}} = 1 + (\lambda_k + up) p^{k+2} \text{ avec } (\lambda_k + up) = \lambda_{k+1}$$

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

Démonstration 14. $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1[p^\alpha]$
 \Rightarrow l'ordre de $1+p$ divise $p^{\alpha-1}$

$$(1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1} \\ \text{Si on avait } 1 + \lambda_{\alpha-2} p^{\alpha-1} \equiv 1[p^\alpha] \\ \Rightarrow p^\alpha | \lambda_{\alpha-2} p^{\alpha-1} \\ \Rightarrow p | \lambda_{\alpha-2} \text{ impossible} \\ \Rightarrow (1+p)^{p^{\alpha-2}} \not\equiv 1[p^\alpha]$$

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

Démonstration 15. Soit $\psi : \mathbb{Z}/p^\alpha \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$
 $[n] \mapsto [n]$

\Rightarrow induit $\psi : (\mathbb{Z}/p^\alpha \mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ morphisme de groupe.
 $(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément x d'ordre $p-1$.
 ψ est surjectif $\Rightarrow \exists y \in (\mathbb{Z}/p^\alpha \mathbb{Z})^\times$ tel que $\psi(y) = x$.
 \Rightarrow l'ordre de y est un multiple de $p-1$.

Si d = l'ordre de y
 $y^d = 1 \Rightarrow \psi(y^d) = \psi(1) = 1$
 et $\psi(y^d) = \psi(y)^d = x^d$
 $\Rightarrow p-1 | d$
 (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. $\mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z}$

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

Lemme 7. Soit $k \in \mathbb{N}$,

$$\exists \mu_k \text{ impair tel que } 5^{2^k} = 1 + 2^{k+2} \mu_k$$

Démonstration 16. *Démonstration de la proposition. Les deux premiers cas sont évidents. Supposons $\alpha \geq 3$.*

$$\psi : (\mathbb{Z}/2^\alpha \mathbb{Z})^\times \rightarrow (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$$

$$\psi(2^\alpha) = 2^{\alpha-1}$$

$$\psi(3) = 3$$

$\Rightarrow 3$ est d'ordre pair. Ordre $(3) = 2d$.

3^d est d'ordre 2.

$$S : (\mathbb{Z}/4\mathbb{Z})^\times \rightarrow (\mathbb{Z}/2^{\alpha-1}\mathbb{Z})^\times [1] \rightarrow [1][3] \rightarrow [3^d]$$

$$S \circ \phi = id$$

$$f : (\mathbb{Z}/2^\alpha \mathbb{Z})^\times \rightarrow \ker(\phi) \times (\mathbb{Z}/4\mathbb{Z})^\times [n] \rightarrow [ns(n)^{-1}, \phi(n)]$$

$$\text{Ordre à gauche} = \text{ordre à droite} = \phi(2^\alpha) = 2^{\alpha-1}$$

$$|Ker(\psi)| = \frac{|(\mathbb{Z}/2^\alpha \mathbb{Z})^\times|}{|(\mathbb{Z}/4\mathbb{Z})^\times|} = 2^{\alpha-2}$$

$$5 \in \ker \psi \text{ et } 5 \text{ est d'ordre } 2^{\alpha-2}$$

$\Rightarrow 5$ engendre $\ker(\phi)$

$(\ker(\phi)) \times (\mathbb{Z}/4\mathbb{Z})^\times$ est engendré par la famille $\{(5,1), (1,3)\}$

$$(5, 1) = f(5)$$

$$(1, 3) = f(3)$$

$\Rightarrow f$ est surjectif.

Comme les deux groupes ont le même ordre, f est une bijection

\Rightarrow c'est un iso.

$$5^{2^{\alpha-2}} = 1 + \mu_{\alpha-3} 2^\alpha$$

$$\equiv 1[2^\alpha]$$

\Rightarrow l'ordre de 5 divise $2^{\alpha-2}$

$$5^{2^k} = 1 + \mu_{\alpha-3} 2^{k+2}, \text{ avec } k < \alpha - 2$$

$$\text{Si c'était } \equiv 1[2^\alpha]$$

$$\Rightarrow 2^\alpha | (2^{k+2} \mu_k + 1 - 1)$$

$$\Rightarrow 2 | 2^{\alpha-k-2} | \mu_k$$

Theorem 4. des restes chinois

Soit $a, b \geq 2$ 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 $n \in \mathbb{N}^*$

$$\text{Si } n = 2^\alpha p_1^{\alpha_1} p_k^{\alpha_k}$$

où $\alpha, \alpha_i \geq 0$ et p_1, \dots, p_k sont premiers, différents deux à deux, alors :

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong$$

$$(\mathbb{Z}/2^\alpha \mathbb{Z})^\times \times (\mathbb{Z}/p_1^{\alpha_1} \mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_k^{\alpha_k} \mathbb{Z})^\times$$

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

$$\text{Si } n \in \ker(f), n \equiv 0[a]$$

$$n \equiv 0[b]$$

$a|n$ et $b|n$

\Rightarrow le ppcm $(a,b) = ab$ divise n .

$$\Rightarrow n \equiv 0 \pmod{ab}$$

$$\Rightarrow [n] = 0$$

$$\text{Si } n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

$$\phi(n) = \phi(p_1^{\alpha_1}) \dots \phi(p_k^{\alpha_k})$$

$$= p_1^{\alpha_1-1}(p_1-1) \dots p_k^{\alpha_k-1}(p_k-1)$$

$$= n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$$

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