Khôlles : Semaine 20

- 12 - 16 Février 2024 -

Sommaire

1 Questions de cours - Groupes A, B, C

1.1 Définitions de sous-groupe, sous-anneau, sous-algèbre

Définition: Sous-groupe

Soit $(G, \star)$, un groupe et $H \subset G$.

On dit que H est un sous-groupe de G si :

- H est non vide
- H est stable par $\star$: $\forall x, y \in H,\ x \star y \in H$
- H est stable par passage au symétrique : $\forall x \in H,\ x^{-1} \in H$

Note:-

Les deux dernières conditions sont équivalentes à vérifier : $\forall x, y \in H,\ x \star y^{-1} \in H$

Définition: Sous-Anneau

Soit $(A, +, \times)$, un anneau et $B \subset A$.

On dit que B est un sous-anneau de A si :

- $(B, +)$ est un sous-groupe de $(A, +)$
- B est stable par $\times$
- $\mathbb{1}_A \in B$ (l'élément neutre pour la loi $\times$)

Définition: Sous-Algèbre

Soit $(A, +, \times, \cdot)$, une $\mathbb{K}$-Algèbre et $B \subset A$.

On dit que B est une sous-Algèbre de A si :

- B est un Sous-Espace vectoriel de A
- B est un sous-anneau de A

Note:-

La deuxième condition peut être remplacée par :

- B est stable pour la loi $\times$
- $\mathbb{1}_A \in B$

1.2 Une intersection de sous-groupes est un sous-groupe. (démo)

Preuve :

Soit $(G,\star)$, un groupe, avec F, H, deux sous-groupes de G. Montrons que $F \cap H$ est un sous-groupe de G :

- $F \cap H$ est non vide, car contient e (F et H étant des sous-groupes, ils héritent naturellement du neutre de la loi $\star$).
- Soient $x, y \in F \cap H$. Alors $x, y \in F$ et $x, y \in H$. Or, F et H sont des sous-groupes, donc $x \star y \in F$ et $x \star y \in H$, d'où $x \star y \in F \cap H$
- Soit $x \in F \cap H$. Alors $x^{-1} \in F \cap H$, car $x \in F \Rightarrow x^{-1} \in F$, ainsi que $x \in H \Rightarrow x^{-1} \in H$

Dès lors, $F \cap H$ est un sous-groupe de G.

1.3 Produit cartésien de deux groupes. C'est un groupe. (démo)

Définition: Produit (direct) de Groupes

Soient $(G,\star), (H,\cdot)$, deux groupes.

Nous munissons naturellement $G \times H$ d'une structure de groupe en posant $\bullet$, loi de composition interne composante par composante. i.e :

$$\forall ((x_1,y_1),(x_2,y_2)) \in (G \times H)^2,\ (x_1,y_1) \bullet (x_2,y_2) = (x_1 \star x_2, y_1 \cdot y_2)$$

Preuve :

- Notons que $G \times H$ est non vide, car G et H étant des groupes, $(e_G, e_H) \in G \times H$
- Soient $(x_1,y_1),(x_2,y_2) \in (G \times H)^2$. alors $x_1 \star x_2 \in G$ et $y_1 \cdot y_2 \in H$, car G et H sont des groupes. Donc $(x_1 \star x_2, y_1 \cdot y_2) = (x_1,y_1) \bullet (x_2,y_2) \in G \times H$
- Idem, soit $(x,y) \in G \times H$. Alors $x^{-1} \in G$ et $y^{-1} \in H$, car G et H sont deux groupes. Donc $(x^{-1},y^{-1}) = (x,y)^{-1} \in G \times H$

(il est immédiat que $(x,y)^{-1} = (x^{-1},y^{-1})$, car avec $(x,y)^{-1} = (u,v)$, $(x,y) \bullet (x,y)^{-1} = e_{G\times H} \Rightarrow (x \star u, y \cdot v) = (e_G, e_H) \Rightarrow u = x^{-1}$ et $v = y^{-1}$)

$(G \times H, \bullet)$ est bien un groupe.

1.4 Définitions de morphisme de groupe, morphisme d'anneau, d'algèbre.

Définition: Morphisme de groupe, d'anneau, d'algèbre

Soient $(G,\star)$ et $(H,\cdot)$ deux groupes. Soit $\varphi : G \to H$, une application.

On dit que φ est un morphisme de groupe si :

$$\forall a,b \in G,\ \ \varphi(a\star b) = \varphi(a)\cdot\varphi(b)$$

Soient $(A,+,\times)$ et $(B,\overline{+},\overline{\times})$, deux anneaux.

On dit de même que $\varphi : A \to B$ est un morphisme d'anneau si :

- φ est un morphisme de groupe
- $\forall a,b \in A,\ \ \varphi(a\times b) = \varphi(a)\overline{\times}\varphi(b)$
- $\varphi(\mathbb{1}_A) = \mathbb{1}_B$

Enfin, soient $(A,+,\times,\cdot)$ et $(B,\overline{+},\overline{\times},\overline{\cdot})$, deux $\mathbb{K}$-Algèbres, et $\varphi : A \to B$ une application.

On dit que $\varphi : A \to B$ est un morphisme d'algèbre si :

- φ est un morphisme d'anneau
- φ est linéaire

1.5 L'image directe et l'image réciproques de sous-groupes par un morphisme de groupe sont des sous-groupes. (démo)

Preuve :

Soient $(G,\star),(H,\cdot)$, deux groupes, ainsi que $G_1 \subset G, H_1 \subset H$, deux sous-groupes. Soit $\varphi : G \to H$, morphisme de groupe.

$G_1 \neq \emptyset$ par définition d'un sous-groupe : $\varphi(G_1) \neq \emptyset$ car $e_G \in G_1$.

$\forall y_1,y_2 \in \varphi(G_1),\ \ \exists x_1,x_2 \in G,\ \ \varphi(x_1) = y_1$ et $\varphi(x_2) = y_2$. Ainsi, $y_1 \cdot y_2^{-1} = \varphi(x_1 \star x_2^{-1})$ et $x_1 \star x_2^{-1} \in G_1$ car G_1 est un sous-groupe. Ainsi, $\varphi(x_1 \star x_2^{-1}) \in \varphi(G_1)$. Dès lors, $\varphi(G_1)$ est un sous-groupe de H.

Pour H_1 : $\varphi(e_G) = e_H$ et $e_H \in H_1$, ainsi, $\varphi^{-1}(H_1) \neq \emptyset$, car contient e_G.

$\forall x_1,x_2 \in \varphi^{-1}(H_1),\ \ \varphi(x_1) \in H_1$ et $\varphi(x_2) \in H_1$. Or, H_1 est un sous-groupe, donc $\varphi(x_1)\cdot\varphi(x_2)^{-1} \in H_1 \Rightarrow \varphi(x_1 \star x_2^{-1}) \in H_1 \Rightarrow x_1 \star x_2^{-1} \in \varphi^{-1}(H_1)$.

1.6 Les sous-groupes de $(\mathbb{Z},+)$. (démo)

Proposition Les sous-groupes de $(\mathbb{Z},+)$

Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les $n\mathbb{Z}$, pour $n \in \mathbb{Z}$

Preuve :

Soit $n \in \mathbb{Z}$, $\quad 0 = 0 \times n \in n\mathbb{Z}$: $n\mathbb{Z}$ est non-vide.
Soient x et $y \in n\mathbb{Z}$, il existe $(k,p) \in \mathbb{Z}^2$ tq $x = kn$ et $y = np$. D'où $x+y = n(k+p) \in n\mathbb{Z}$.
Et, $-x = n(-k) \in n\mathbb{Z}$.

$n\mathbb{Z}$ est stable par somme et par opposé. $n\mathbb{Z}$ est alors un sous-groupe de $\mathbb{Z}$

Soit H, un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, $H = 0\mathbb{Z}$. Sinon, il existe $x \in H$, $x \neq 0$.
Alors, H contient un élément strictement positif : Si $x>0$, x convient.
Sinon, $-x$ convient ($-x \in H$ car H est un sous-groupe de $\mathbb{Z}$ donc est stable par opposé).
Notons $n = \min(\mathbb{N}^* \cap H)$ (Partie non-vide de $\mathbb{N}$ donc admet un plus petit élément).
Montrons que $H = n\mathbb{Z}$:

$0 \in H$ car c'est un sous-groupe de $\mathbb{Z}$, $n \in H$ par hypothèse.
$2n = n+n \in H$ car H est stable par somme. $3n = 2n+n \in H$...
Par récurrence immédiate, $np \in H$ pour tout $p \in \mathbb{N}$. Or, si $p<0$, $np = -n(-p) \in H$ car H est stable par opposé.
Finalement, $n\mathbb{Z} \subset H$.

Réciproquement, soit $x \in H$, $x \neq 0$. D'après le principe de division euclidienne : il existe $p \in \mathbb{Z}$ et $r \in [\![0; n-1]\!]$, tels que $x = np + r$. Or, $x \in H$, $np \in H$, et H est un sous-groupe de $\mathbb{Z}$ donc est stable par somme (et par inverse) : $x - np = r \in H$. Or, si $r \neq 0$, $0 \leqslant r<n$ et $n = \min(\mathbb{N}^* \cap H)$. Ce qui est absurde. Donc $x \in n\mathbb{Z}$, $H \subset n\mathbb{Z}$:

$$H = n\mathbb{Z}$$

1.7 Sous-groupe engendré par une partie, sous-groupe engendré par un élément.

Définition

Soit $(G,\star)$, un groupe. Soit $A \subset G$.

On appelle Sous-groupe engendré par A le groupe : $\mathrm{Gr}(A) = \bigcap_{\substack{H \text{ sous-groupe} \\ A \subset H}} H$.

Cet ensemble :

- Existe
- Est un groupe
- Est le plus petit sous-groupe de G (pour l'inclusion) contenant A.

Preuve

- G **est un sous-groupe de** G **: L'intersection existe**
- **Gr**(A) **est une intersection de sous-groupes : c'est un sous-groupe.**
- $\forall H_0 \subset G$**, sous-groupe tel que** $A \subset H_0$**, alors Gr**$(A) \subset H_0$ **par définition.**

:

1.8 Caractérisation de l'injectivité d'un morphisme de groupes par le noyau. (démo)

Proposition

Soient $(G,\star)$ et $(H,\cdot)$, deux groupes et $\varphi : G \to H$, morphisme de groupe.

$$\varphi \text{ est injective} \iff \text{Ker}(\varphi) = \{e_G\}$$

Preuve :

Supposons que φ est injective. Alors, par définition d'un morphisme de groupe : $\varphi(e_G) = e_H$. Or, φ est injective, et e_G convient : e_G est donc le seul élément envoyé sur e_H : $\text{Ker}(\varphi) = \{e_G\}$

Réciproquement, supposons que $\text{Ker}(\varphi) = \{e_G\}$. Alors, soient $x_1, x_2 \in G$, tels que $\varphi(x_1) = \varphi(x_2)$. Dès lors :

$$\begin{aligned} \varphi(x_1) \cdot \varphi(x_2)^{-1} &= e_H \\ \varphi(x_1 \star x_2^{-1}) &= e_H \end{aligned}$$

Or, $\text{Ker}(\varphi) = \{e_G\}$, donc $x_1 \star x_2^{-1} = e_G \Rightarrow x_1 = x_2$: φ est alors injective.

1.9 Définition d'un idéal et lien avec les noyaux des morphismes d'anneau.

Définition: Idéal

Soit $(A,+,\times)$, un anneau Commutatif et $I \subset A$.

On dit que I est un idéal de A si :

- I est un sous-groupe de $(A,+)$
- I est absorbant pour $\times$: $\forall x \in A, \forall a \in I,\ a \times x \in I$

Proposition Lien avec les noyaux des morphismes d'anneaux

Soient $(A,+,\times)$ et $(B,\overline{+},\overline{\times})$, deux anneaux et $\varphi : A \to B$, un morphisme d'anneau.

Alors, $\mathrm{Ker}(\varphi)$ est un idéal.

Preuve :

Soit $I = \mathrm{Ker}(\varphi)$. Alors, $(I,+)$ est un sous-groupe de A :

- $0_A \in \mathrm{Ker}(\varphi) = I$ par définition d'un morphisme d'anneau
- $\forall a,b \in I,\ \varphi(a-b) = \varphi(a)\overline{-}\varphi(b) = 0_B$

  Soit $x \in I,\ a \in A$. Alors, $\varphi(x \times a) = \varphi(x)\overline{\times}\varphi(a) = 0_B \overline{\times} \varphi(a)$.
  Or, le neutre est absorbant pour le produit : $\varphi(a \times x) = 0_B$ donc $a \times x \in I \Rightarrow$ I est un idéal.

2 Questions de cours, groupes B et C

2.1 L'ordre d'un élément, dans un groupe fini, divise le cardinal du groupe. (démo dans le cas abélien)

Proposition

Soit $(G,\star)$, groupe fini.
Alors, tout élément de G est d'ordre fini. De plus, $\forall a \in G,\ O(a) \,|\, |G|$

Preuve* Cas de G abélien *:

Lemme

$\varphi_a : \begin{cases} G \to G \\ g \mapsto a \star g \end{cases}$ est bijective. (n'est pas un morphisme de groupe dans le cas général).

On peut aisément trouver φ^{-1}, ou bien : $\forall g_1, g_2 \in G,\ \varphi(g_1) = \varphi(g_2) \Rightarrow a \star g_1 = a \star g_2 \Rightarrow g_1 = g_2$. Or, G est fini, donc injective $\iff$ bijective.

Posons $n = |G|$, ainsi que $G = \{g_1, \ldots, g_n\}$.

Considérons $x = g_1 \star \cdots \star g_n$. Alors, $x = \varphi(g_1) \star \cdots \star \varphi(g_n)$ car φ est bijective et G est abélien.

Alors, $x = a \star g_1 \star a \star g_2 \star \cdots \star a \star g_n = a^n \star g_1 \star \cdots \star g_n = a^n x$.

Dès lors, $a^n = e_G \Rightarrow O(a) \,|\, n = |G|$

2.2 La somme de deux idéaux est un idéal. (démo)

Proposition

Soit $(A,+,\times)$, anneau commutatif. Soient I_1, I_2, deux idéaux de A.

On note $I_1+I_2=\{a+b \mid a\in I_1,\ b\in I_2\}=\{y\in A,\ \mid \exists (a,b)\in I_1\times I_2,\ y=a+b\}$.

Alors, I_1+I_2 est un idéal de A

Preuve :

$I_1+I_2\neq\emptyset$ car $0\in I_1$ et I_2, donc $0\in I_1+I_2$.

$\forall a,b\in I_1+I_2,\ \exists \alpha,\beta,\gamma,\delta\in I_1^2\times I_2^2,\ a=\alpha+\gamma$ et $b=\beta+\delta$.

Alors, $a+b=(\alpha+\beta)+(\gamma+\delta)\in I_1+I_2$ car $\alpha,\beta\in I_1$ et $\gamma,\delta\in I_2$.

$\forall x\in I_1+I_2,\ \forall z\in A,\ \exists (a,b)\in I_1\times I_2,\ x=a+b$.

Dès lors, $xz=(a+b)z=az+bz$. Or, I_1 et I_2 sont deux idéaux : $az\in I_1$ et $bz\in I_2\Rightarrow xz\in I_1+I_2\Rightarrow I_1+I_2$ est un idéal de $(A,+,\times)$

2.3 Dans $(\mathbb{Z},+)$, lien entre PGCD et somme d'idéaux. (démo)

Note:-

Les idéaux de $(\mathbb{Z},+,\times)$ sont exactement les $n\mathbb{Z}$ avec $n\in\mathbb{Z}$.

Définition

Soient $a,b\in\mathbb{Z}^*$, alors, $\exists! n\in\mathbb{N}^*,\ a\mathbb{Z}+b\mathbb{Z}=n\mathbb{Z}$

On appelle ce n le PGCD de a et b, on note $n=a\wedge b$

Proposition

Cette notion de PGCD coïncide avec le PGCD déjà défini sur $\mathbb{Z}$

Preuve :

Notons n_1 le nouveau PGCD, et n_2 l'ancien PGCD.

D'après le théorème de Bézout : $\exists u,v\in\mathbb{Z},\ au+bv=n_2$.

Or, $au+bv\in a\mathbb{Z}+b\mathbb{Z}\Rightarrow n_2\in n_1\mathbb{Z}\Rightarrow n_1\mid n_2$.

Par définition, $n_2\mid a$ et $n_2\mid b\Rightarrow \exists c,d\in\mathbb{Z},\ a=n_2c,\ b=n_2d$.

$n_1\in n_1\mathbb{Z}\Rightarrow n_1\in a\mathbb{Z}+b\mathbb{Z}\Rightarrow \exists u,v\in\mathbb{Z},\ n_1=au+bv=n_2(cu+dv)\Rightarrow n_2\mid n_1\Rightarrow n_2=n_1$

2.4 Eléments inversibles de $(\mathbb{Z}/n\mathbb{Z},+,\times)$. (démo)

Proposition

Soit $n \in \mathbb{N}^*$, soit $k \in \mathbb{Z}$. Alors :

$$\begin{aligned} \overline{k} \text{ est inversible dans } (\mathbb{Z}/n\mathbb{Z},+,\times) &\iff k \wedge n = 1 \\ &\iff \overline{k} \text{ est un générateur de } (\mathbb{Z}/n\mathbb{Z},+) \end{aligned}$$

Preuve :

$\overline{k}$ est inversible donne l'existence de $p \in \mathbb{Z}$, tel que $\overline{k} \times \overline{p} = \overline{1} \Rightarrow \overline{kp} = \overline{1}$

Ainsi, $kp - 1 \in n\mathbb{Z}$, donc $\exists q \in \mathbb{Z},\ kp - 1 = nq \Rightarrow kp - nq = 1$.
Par le théorème de Bézout : $k \wedge n = 1$

Réciproquement : Si $k \wedge n = 1$, par le théorème de Bézout : $\exists u, v \in \mathbb{Z},\ \overline{ku + nv} = \overline{1} \Rightarrow \overline{ku} + \overline{0} = \overline{1}$
$\Rightarrow \exists u \in \mathbb{Z},\ \overline{k} \times \overline{u} = \overline{1}$.

Ainsi, $\overline{k}$ est inversible.

2.5 Générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$. (démo)

Proposition

Soit $n \in \mathbb{N}^*$:

- $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique
- Soit $k \in \mathbb{Z}$. Alors $\overline{k}$ est générateur de $(\mathbb{Z}/n\mathbb{Z},+)$ si et seulement si $k \wedge n = 1$

Preuve :

- $(\mathbb{Z}/n\mathbb{Z},+)$ est fini, de cardinal n. Or, $\mathrm{Gr}(\{\overline{1}\}) = \{\overline{0}, \overline{1}, \overline{1+1}, \ldots, \overline{n-1}\} = \mathbb{Z}/n\mathbb{Z}$
- Par le théorème de Bézout : Supposons $\overline{k}$ générateur de $\mathbb{Z}/n\mathbb{Z}$. Alors, $\mathrm{Gr}(\overline{k}) = \mathbb{Z}/n\mathbb{Z}$. En particulier :
  $\exists p \in \mathbb{Z},\ \overline{kp} = \overline{1} \Rightarrow \overline{kp-1} \in n\mathbb{Z}$.

  Dès lors, $\exists q \in \mathbb{Z},\ kp - 1 = nq \Rightarrow kp - nq = 1 \Rightarrow k \wedge n = 1$ par théorème de Bézout.

  Réciproquement, par théorème de Bézout : $\exists p, q \in \mathbb{Z},\ kp + nq = 1 \Rightarrow \overline{pk} + \overline{qn} = \overline{1}$

  Donc, $\overline{uk} + \overline{0} = 1$, donc $\overline{k}$ engendre $\overline{1}$, donc $\mathbb{Z}/n\mathbb{Z}$: $\mathrm{Gr}(\overline{k}) = \mathbb{Z}/n\mathbb{Z}$

2.6 Théorème des restes chinois. (démo)

Théorème des Restes chinois
Soient $n, m \in \mathbb{Z}^*$ tels que $n \wedge m = 1$

Alors, $(\mathbb{Z}/(n \times m)\mathbb{Z}, +, \times)$ est naturellement isomorphe à $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \times)$

Théorème des Restes chinois (V.2)
Soient $n, m, a, b \in \mathbb{Z}$ tels que $n \wedge m = 1$

Alors, $\exists! c \in [\![0, mn-1]\!]$, $\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases} \iff x \equiv c[nm]$

Preuve :

Si $k \in \mathbb{Z}$, on note $\overline{k}$ sa classe dans $\mathbb{Z}/nm\mathbb{Z}$, on note également $\overline{\overline{k}}$ sa classe dans $\mathbb{Z}/m\mathbb{Z}$ et $\overline{\overline{k}}$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$

Considérons $\varphi : \begin{cases} \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \\ \overline{k} \mapsto (\overline{\overline{k}}, \overline{\overline{k}}) \end{cases}$

1. φ est correctement définie :
   $\forall k_1, k_2 \in \mathbb{Z}$ tels que $\overline{k_1} = \overline{k_2}$: $\exists p \in \mathbb{Z},\ k_1 - k_2 = nmp$, Alors $\overline{\overline{k_1 - k_2}} = \overline{\overline{pmn}} = \overline{\overline{0}}$ car $\overline{\overline{m}} = 0$

   Par le même raisonnement avec $\overline{\overline{\overline{k_1 - k_2}}}$, on trouve $\varphi(k_1) = \varphi(k_2)$

2. φ est un morphisme d'anneau :
   $\forall \overline{k_1}, \overline{k_2} \in \mathbb{Z}/n\mathbb{Z}$: $\varphi(\overline{k_1} + \overline{k_2}) = \varphi(\overline{k_1 + k_2}) = (\overline{\overline{k_1 + k_2}}, \overline{\overline{\overline{k_1 + k_2}}}) = (\overline{\overline{k_1}} + \overline{\overline{k_2}}, \overline{\overline{k_1}} + \overline{\overline{k_2}}) = \varphi(\overline{k_1}) + \varphi(\overline{k_2})$

   De plus : $\varphi(\overline{k_1} \times \overline{k_2}) = \varphi(\overline{k_1 \times k_2}) = (\overline{\overline{k_1 \times k_2}}, \overline{\overline{\overline{k_1 \times k_2}}}) = (\overline{\overline{k_1}} \times \overline{\overline{k_2}}, \overline{\overline{k_1}} \times \overline{\overline{k_2}}) = \varphi(\overline{k_1}) \times \varphi(\overline{k_2})$

   Finalement, $(\overline{\overline{1}}, \overline{\overline{1}})$ est le neutre pour $\times$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

3. Utilisons le fait que φ soit un morphisme de groupes :

   $\forall \overline{k} \in \mathrm{Ker}(\varphi) : \varphi(\overline{k}) = (\overline{\overline{0}}, \overline{\overline{0}}) \Rightarrow \overline{\overline{k}} = \overline{\overline{0}}$ et $\overline{\overline{k}} = \overline{\overline{0}}$.

   $\Rightarrow k \in m\mathbb{Z},\ k \in n\mathbb{Z}$
   $\Rightarrow mn \mid k$ car $m \wedge n = 1$ d'après le théorème de Gauß
   $\Rightarrow \overline{k} = \overline{0} \Rightarrow \mathrm{Ker}(\varphi) = \{\overline{0}\}$
   $\Rightarrow \varphi$ est Injective

4. $\mathrm{Card}(\mathbb{Z}/mn\mathbb{Z}) = mn$ et $\mathrm{Card}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) = mn \Rightarrow$ φ est bijective car injective entre deux ensembles de même cardinal.

2.7 Définition de l'indicatrice d'Euler, propriétés et calcul. (démo)

Définition: Indicatrice d'Euler

Soit $n \in \mathbb{N}^*$. On note :

$$\begin{aligned}\varphi(n) &= \text{Card}\{k \in [\![1,n]\!] \mid k \wedge n = 1\} \\ &= \text{Card}\,(\mathbb{Z}/n\mathbb{Z})^* \quad (n \geqslant 2) \\ &= \text{Nombres de générateurs de } (\mathbb{Z}/\,n\mathbb{Z}, +)\end{aligned}$$

Proposition

1. Soient $m, n \in \mathbb{N}^*$, si m et n sont Copremiers, alors $\varphi(nm) = \varphi(n) \times \varphi(m)$
2. $\forall p \in \mathbb{P},\ \forall k \in \mathbb{N}^*,\ \varphi(p^k) = (p-1)p^{k-1}$

Preuve :

1. D'après le théorème des restes chinois : $\mathbb{Z}/nm\mathbb{Z} \sim \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
   Donc, $(\mathbb{Z}/nm\mathbb{Z})^*$ est naturellement isomorphe à $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.

   Lemme permettant d'affirmer l'isomorphisme précédent
   Soit $\varphi : A \to B$ un isomorphisme. Alors $a \in A$ est inversible si et seulement si $\varphi(a) = b$ est inversible.

   Soit $(a,b) \in A \times B$, (a,b) inversible dans $A \times B \iff a$ et b inversibles.

   Dès lors, $\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/n\mathbb{Z})^*| \times |(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m) \times \varphi(n)$

2. Soit $p \in \mathbb{R},\ k \in \mathbb{N}^*$. Posons $A = \{n \in [\![1,p^k]\!] \mid n \wedge p^k \neq 1\} = \{n \in [\![1,p^k]\!] \mid p \mid n\} = \{pq \mid q \in [\![1,p^{k-1}]\!]\}$

   Dès lors, $\text{Card}(A) = p^{k-1}$. Posons également $B = \{n \in [\![1,p^k]\!] \mid n \wedge p^k = 1\}$. Donc $B = [\![1,p^k]\!] \setminus A$.

   Ainsi, $\varphi(p^k) = \text{Card}(B) = p^k - \text{Card}(A) = p^{k-1}(p-1)$

Proposition

Soit $n \in \mathbb{N}^*$

$$\varphi(n) = n \times \prod_{p \in \mathrm{Div}_p(n)} \left(1 - \frac{1}{p}\right) \quad \text{où } \mathrm{Div}_p(n) \text{ sont les diviseurs premiers de } n$$

Preuve :

D'après la propriété précédente :

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}) \\
&= \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1} \\
&= n \times \frac{(p_1 - 1) \times \cdots \times (p_k - 1)}{p_1 \times \cdots \times p_k} \\
&= n \times \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

2.8 Théorème d'Euler. (démo)

Théorème d'Euler

Soit $n \in \mathbb{N}$, $(n \geqslant 2)$, $a \in \mathbb{Z}$.

Si a est premier avec n, alors $a^{\varphi(n)} \equiv 1[n]$.

De plus, si n est premier, $\varphi(n) = n - 1$, donc $a \wedge n = 1 \Rightarrow a^{n-1} \equiv 1[n]$
(pour a quelconque : $a^n \equiv a[n]$)

Preuve :

$a \wedge n = 1 \Rightarrow \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Or, $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe pour $\times$, de cardinal $\varphi(n)$ (cardinal fini).

Donc, $\overline{a}$ est d'ordre fini et $O(\overline{a}) \mid \varphi(n) \Rightarrow a^{\varphi(n)} = \overline{1} \left(= \overline{a}^{O(\overline{a})^k}\right) \Rightarrow a^{\varphi(n)} \equiv 1[n]$

2.9 Définition du pgcd dans $\mathbb{R}[X]$.

Définition

Soient $P, Q \in \mathbb{K}[X]$, avec P et $Q \neq 0$

1. Alors, $P\mathbb{K}[X]$ et $Q\mathbb{K}[X]$ sont des idéaux, donc $P\mathbb{K}[X] + Q\mathbb{K}[X]$ est un idéal.
   Alors, $\exists! R \in \mathbb{K}[X]$, tel que R soit unitaire et $P\mathbb{K}[X] + Q\mathbb{K}[X] = R\mathbb{K}[X]$. On pose alors par définition $R = \text{PGCD}(P, Q)$
2. Cette notion de PGCD Coïncide avec celle de première année.

Preuve :

$P \in P\mathbb{K}[X] + Q\mathbb{K}[X] = R\mathbb{K}[X] \Rightarrow R \mid P$. Idem, $R \mid Q$
Ainsi, $R \mid (P \wedge Q)$

Notons $T = P \wedge Q$. $P\mathbb{K}[X] + Q\mathbb{K}[X] = R\mathbb{K}[X] \Rightarrow R \in P\mathbb{K}[X] + Q\mathbb{K}[X]$.
Ainsi, $\exists U, V \in \mathbb{K}[X]$ tels que $R = PU + QV$. Or, $T \mid P$ et $T \mid Q$, donc $T \mid R = PU + QV$.

Ainsi, $R \mid T$ et $T \mid R$, donc $R = T$ car sont tous deux unitaires.

2.10 Théorèmes de Gauß et de Bézout dans $\mathbb{R}[X]$. (démo)

Théorème de Bézout

Soient $P, Q \in \mathbb{K}[X]$.

1. $P \wedge Q = 1 \iff \exists U, V \in \mathbb{K}[X],\ PU + QV = 1$
2. On note $R = P \wedge Q$. Alors, $\exists U, V \in \mathbb{K}[X],\ PU + QV = R$

Preuve :

1. $P \wedge Q = 1 \Rightarrow P\mathbb{K}[X] + Q\mathbb{K}[X] = \mathbb{K}[X]$. Or, $1 \in \mathbb{K}[X] \Rightarrow \exists U, V \in \mathbb{K}[X],\ PU + QV = 1$

   Réciproquement, s'il existe $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1$, alors $1 \in P\mathbb{K}[X] + Q\mathbb{K}[X]$ qui est un idéal, donc $P\mathbb{K}[X] + Q\mathbb{K}[X] = \mathbb{K}[X] \Rightarrow P \wedge Q = 1$
2. On note $R = P \wedge Q$. Alors $P\mathbb{K}[X] + Q\mathbb{K}[X] = R\mathbb{K}[X] \Rightarrow \exists U, V \in \mathbb{K}[X],\ PU + QV = R$

Théorème de Gauß
Soient $A, B, C \in \mathbb{K}[X]$. Si $A \mid BC$ et $A \wedge B = 1$, alors $A \mid C$

Preuve :

D'après le théorème de Bézout, $\exists U, V \in \mathbb{K}[X],\ AU + BV = 1$.

Ainsi, $AUC + BVC = C$. Or, $A \mid BC \Rightarrow \exists P \in \mathbb{K}[X], AP = BC$.
Ainsi, $AUC + APV = C \Rightarrow A(UC + PV) = C$, donc $A \mid C$

3 Questions de Cours du groupe C uniquement

3.1 Un groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$. (démo)

Preuve :

Soit $(G, \star)$, groupe monogène infini engendré par $a \in G$.

Nous avons alors $\forall k_1, k_2 \in \mathbb{Z},\ a^{k_1} = a^{k_2} \iff k_1 = k_2$, car si $k_1 \neq k_2$ et $a^{k_1} = a^{k_2}$,

alors $a^{k_1 - k_2} = e_G \Rightarrow$ a d'ordre fini $\Rightarrow$ G fini : Absurde.

Il suffit de poser le morphisme $\varphi : \begin{cases} \mathbb{Z} \to G \\ k \mapsto a^k \end{cases}$.

On vérifie facilement :

- $\forall k_1, k_2 \in \mathbb{Z},\ \varphi(k_1 + k_2) = a^{k_1 + k_2} = a^{k_1} \star a^{k_2} = \varphi(k_1) \star \varphi(k_2)$
- φ est injective : Déjà fait
- φ est surjective, car a est générateur de G.

Alors $(G, \star)$ et $(\mathbb{Z}, +)$ sont isomorphes.

3.2 Un groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$. (démo)

Preuve :

$(G,\star)$ est cyclique : Il est donc monogène (tel que $G = \mathrm{Gr}(\{a\})$ pour $a \in G$)

Il existe de plus $n \in \mathbb{Z}$ tel que $a^n = e_G$ (tel que $O(a) = n$). Alors, $G = \{e, a, a^2, \dots, a^{n-1}\}$.

Posons $\varphi : \begin{cases} (\mathbb{Z}/n\mathbb{Z},+) \to (G,\star) \\ \overline{k} \mapsto a^k \end{cases}$

Montrons que φ est correctement définie (les points suivants sont identiques à la démonstration précédente): Soient $k_1, k_2 \in \mathbb{Z}$, tels que $\overline{k_1} = \overline{k_2}$.

Alors, $k_1 - k_2 \in n\mathbb{Z} \Rightarrow \exists q \in \mathbb{Z},\ k_1 - k_2 = nq$, donc $a^{k_1} = a^{k_2+nq} = a^{k_2} \star a^{nq} = a^{k_2}$
$\Rightarrow$ φ est correctement définie.

3.3 L'ordre d'un élément, dans un groupe fini, divise le cardinal du groupe. (démo dans le cas général, non faite en classe)

Preuve* Démo personnelle, signalez les erreurs s'il y en a! *:

Soit $H \subset G$ un sous-groupe. Pour $x, y \in G$, on définit la relation $\mathscr{R}$, telle que $x\mathscr{R}y$ si $x^{-1}y \in H$.

Montrons que $\mathscr{R}$ est une relation d'équivalence :

- Réflexivité : $\forall x \in G,\ x^{-1}x = e_G \in H$ par définition d'un sous-groupe
- Symétrie : $\forall x, y \in G$ tels que $x\mathscr{R}y$, alors $x^{-1}y \in H$. Or, $\left(x^{-1}y\right)^{-1} \in H$ car H est un sous-groupe. Alors, $y^{-1}x \in H \Rightarrow\ y\mathscr{R}x$.
- Transitivité : $\forall x, y, z \in G$, tels que $x\mathscr{R}y$ et $y\mathscr{R}z$: Alors $xy^{-1} \in H$ et $yz^{-1} \in H$. Alors, puisque H est un sous-groupe, ce dernier est stable par composition : $xy^{-1}yz^{-1} = xz^{-1} \in H$. Ainsi, $x\mathscr{R}z$

$\mathscr{R}$ est alors une relation d'équivalence.

Montrons que toute les classes d'équivalence de $\mathscr{R}$ ont le même cardinal.

Soient C_1, C_2, deux classes (qu'on suppose distinctes) de $\mathscr{R}$. Alors, $\exists a \in C_1$ et $b \in C_2$, tels que $x \notin C_2$ et $y \notin C_1$.

Posons $\varphi_{(a,b)} : \begin{cases} C_1 \to C_2 \\ x \mapsto xa^{-1}b \end{cases}$.

Montrons que $\varphi_{(a,b)}$ est bien définie : Soit $x \in C_1$. Alors, $\varphi(x) = xa^{-1}b$, et cet élément est en relation avec b : $xa^{-1}bb^{-1} = xa^{-1} \in H$ car x est dans la classe de a.

De plus, $\varphi_{(a,b)}$ est une bijection, nous pouvons expliciter sa réciproque $\varphi_{(a,b)}{}^{-1} : \begin{cases} C_2 \to C_1 \\ y \mapsto yb^{-1}a \end{cases}$.

Soient $x \in C_1$ et $y \in C_2$.

Alors, ${\varphi_{(a,b)}}^{-1}(\varphi_{(a,b)}(x)) = xa^{-1}bb^{-1}a = x$

et $\varphi_{(a,b)}({\varphi_{(a,b)}}^{-1}(y)) = yb^{-1}aa^{-1}b = y$

Ainsi, ces deux classes d'équivalences possèdent le même cardinal par l'existence d'une bijection entre ces deux ensembles. (car G est fini, tout sous groupe l'est également). Donc toutes les classes d'équivalences de $\mathscr{R}$ sont de même cardinal fini.

En particulier, nous avons pour la classe de l'élément neutre : $x \in \overline{e} \iff ex^{-1} \in H \iff x^{-1} \in H \iff x \in H$ car H est un sous-groupe.

Ainsi, $\overline{e} = H$, donc $\text{Card}(\overline{e}) = |H|$: toute classe d'équivalence de $\mathscr{R}$ est de cardinal $|H|$.

Par définition des classes d'équivalences, ces dernières forment une partition de G, ainsi, puisque G est fini, il existe un nombre fini de classes d'équivalences (On note P cette partition). Or, ces classes sont toutes de cardinal H :

$$|G| = \sum_{p \in P} |p| = \sum_{p \in P} |H| = |H| \times |P|$$

Ainsi, $|H| \,|\, |G|$. Il ne reste qu'à appliquer avec $H = \text{Gr}(\{a\})$.