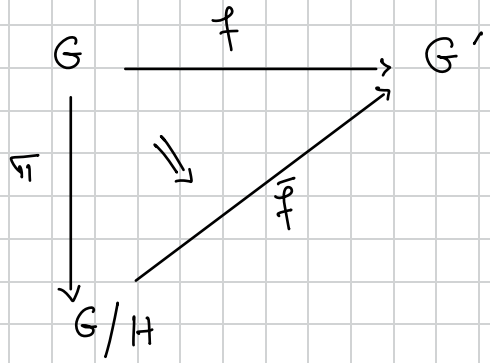


$(G,*) \xrightarrow{f} (G',\#)$ si $\forall\ (x,y) \in G \cdot G$,

$$f(x*y) = f(x) \# f(y)$$

Théorème (Cayley)

$$G \simeq T < \mathfrak{S}_G .$$

G : groupe

Pour g fixé dans G ,

$$\varphi_g : G \longrightarrow G \quad \text{bijection}$$
$$x \longmapsto gx .$$

mais (φ_g n'est pas un morphisme de groupes car

$$\varphi_g(1_G) = g \ )$$

$$\varphi : G \longrightarrow \mathfrak{S}_G \qquad \text{un morphisme de groupes}$$
$$g \longmapsto \varphi_g$$

En effet, $\forall\, x \in G$,

- $$\varphi(gg')(x) = \varphi_{gg'}(x) = (gg')x = g(g'x)$$
$$= \varphi_g(\varphi_{g'}(x))$$
$$= \varphi_g \circ \varphi_{g'}(x)$$

$\Rightarrow \quad \varphi(gg') = \varphi_g \circ \varphi_{g'}$.

- φ est injective : si $g \in \ker \varphi \Rightarrow \varphi_g = id_G \ \forall x \in G$

$\varphi_g(x) = gx = x$; en prenant $x = 1_G$

$\Rightarrow \quad g = 1_G$.

$\Rightarrow$ φ est un morphisme de G sur son image $Im(\varphi)$, qui est un sous-groupe de $\mathfrak{S}_G$.

Théorème (Critère du produit direct)

$$G \simeq G_1 \times G_2 \iff H_1, H_2 < G \ /$$

1. $H_1 \simeq G_1$ et $H_2 \simeq G_2$
2. $\forall h_1 \in H_1$ et $h_2 \in H_2$, $h_1 h_2 = h_2 h_1$
3. $H_1 \cap H_2 = \{ 1_G \}$
4. $G = H_1 H_2 = \{ h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2 \}$

Def : si G/H est fini $\Rightarrow$

$$|G/H| = [G : H]$$ ↖ l'indice de H dans G.

Définition :

$$xHx^{-1} = \{ xhx^{-1} \mid h \in H \}.$$

Prop : $H < G$

1. $\forall x \in G, \quad xHx^{-1} = H \iff$
2. $\forall x \in G, \quad xHx^{-1} \subset H \iff$
3. $\forall x \in G, \quad xH = Hx$

Prop :

si $[G : H] = 2 \Rightarrow H \triangleleft G$

---

si $[G : H] = 2$ on a :

$$G = H \cup xH$$

$\forall x \in G$; $x \notin H$

De même :

$$G = H \cup Hx$$

$\forall x \in G$; $x \notin H$

$\Rightarrow xH = Hx$. L'autre $1_G H = H = H 1_G$

$\Rightarrow H \triangleleft G$.

Prop :

soit $G \xrightarrow{f} G'$ (G groupe, G' groupe)

1. si $H' \lhd G' \Rightarrow f^{-1}(H') \lhd G$. En particulier

$$\ker f \lhd G$$

2. si $H \lhd G$ et si $f \twoheadrightarrow \Rightarrow f(H) \lhd G'$

---

soit $H' \lhd G'$. $f^{-1}(H') < G$.

$f^{-1}(H') \lhd G$?

soit $x \in G$, on veut

$$x f^{-1}(H') x^{-1} \subset f^{-1}(H').$$

soit $y \in f^{-1}(H')$. Il faut montrer que $xyx^{-1} \in f^{-1}(H')$

i.e $f(xyx^{-1}) \in H'$. Or, comme $f \twoheadrightarrow$

$$\Rightarrow f(xyx^{-1}) = f(x) f(y) f(x)^{-1} \in H'$$

($f(y) \in H' \lhd G'$)

$$\sim \quad /\!/$$

$f(x) f(y) f(x)^{-1} \in H' \Rightarrow f^{-1}(H) \lhd G$.

soit $H \triangleleft G$ et supposons que $f \twoheadrightarrow$.

$f(H) < G'$.

$$f(H) \triangleleft G' \ ?$$

soit $y \in G'$. On veut $x f(H) x^{-1} \subset f(H)$.

Comme $f \twoheadrightarrow$, $\exists\, x \in G \ / \ f(x) = y$.

$\Rightarrow f(x^{-1}) = f(x)^{-1} = y^{-1}$.

soit $z \in H \Rightarrow y f(z) y^{-1} = f(\underbrace{x z x^{-1}}) \in f(H)$

$\in H \triangleleft G$

$f \twoheadrightarrow$

$\Vert$

$f(H) \triangleleft G'$.

Groupe quotient.

$G \xrightarrow{\pi} G/H$: surjection canonique

$x \longmapsto xH$

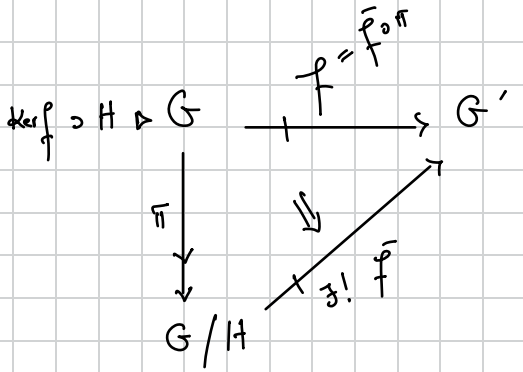
Remarque :

si $H < G$ (abelien)

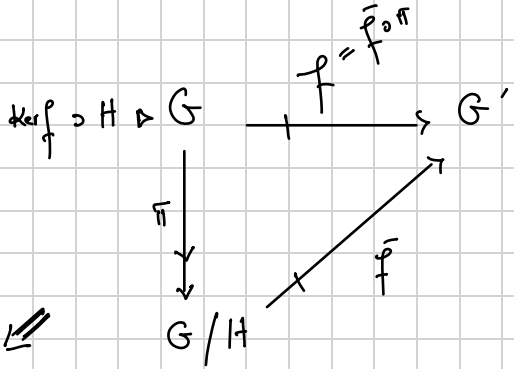
$\Downarrow$

$H \trianglelefteq G$.

Théorème (factorisation)



Théorème (isomorphisme)



1. $\bar{f} \hookrightarrow \Leftrightarrow f \twoheadrightarrow$

2. $\bar{f} \hookrightarrow \Leftrightarrow H = \ker f$. En partie : $G/\ker f \simeq \operatorname{Im} f$.

III. G est dit simple s'il n'a pas de sous-groupe normal non trivial ie distinct de $\{1_G\}$ et G.

Exemple :

$|G| = p \Rightarrow G$ est simple

($|G|$: groupe ; p : premier)

Sous-groupes d'un groupe quotient.

Théorème : $H \triangleleft G$.

$$G \xrightarrow{\pi} G/H.$$

$$\Rightarrow \varphi : \{Y < G \mid H \subset Y\} \longrightarrow \{W < G/H\}$$

$$Y \longmapsto \pi(Y)$$

est une bijection.

Exemple : les sous-groupes de $(\mathbb{Z}/8\mathbb{Z}, +)$ sont :

$\mathbb{Z}/8\mathbb{Z}$, $2\mathbb{Z}/8\mathbb{Z}$, $4\mathbb{Z}/8\mathbb{Z}$, $8\mathbb{Z}/8\mathbb{Z}$ $(= \{0\})$.

Prop : soit $H \triangleleft G$

soit $H \subset K < G$

$$\Downarrow$$

$$K/H \triangleleft G/H \iff K \triangleleft G .$$

Produit semi-direct.

Théorème (produit direct).

soit $H_1, H_2 < G$ /

1. $H_1 \triangleleft G$ et $H_2 \triangleleft G$
2. $H_1 \cap H_2 = \{ 1_G \}$
3. $G = H_1 H_2$

$$\Downarrow$$

$$G \simeq H_1 \times H_2$$

Théorème (produit semi-direct).

$H_1, H_2 < G$ /

1. $H_1 \lhd G$
2. $H_1 \cap H_2 = \{1_G\}$
3. $G = H_1 H_2$

$$\Leftrightarrow$$

$$G = H_1 \rtimes H_2$$

Prof : soit $G = H_1 \rtimes H_2$.

$H_1 < G$, $H_2 < G$

Notons $G' = H_1 \times H_2$

Il est muni de la loi interne suivante :

$$(h_1, h_2) * (h_1', h_2') = (h_1 h_2 h_1' h_2^{-1}, h_2 h_2')$$

$\Rightarrow (G', *)$ est un groupe. $G' \simeq G$.

$$\begin{array}{ccc} G' & \longrightarrow & G \\ (h_1, h_2) & \longmapsto & h_1 h_2 \end{array}$$

Sous-groupes distingués.

Prop : $H < G$, les énoncés suivants sont tous équivalents :

1. $gH = Hg \quad \forall\, g \in G$;
2. $gHg^{-1} = H \quad \forall\, g \in G$;
3. $gHg^{-1} \subset H \quad \forall\, g \in G$.

Preuve : $1 \Rightarrow 2$: $(gH)g^{-1} = (Hg)g^{-1} = H \quad \forall\, g \in G$

$2 \Rightarrow 3$: clair

$3 \Rightarrow 1$: $gH = (gHg^{-1})g \subset Hg$

$Hg = g(g^{-1}Hg) \subset gH \quad \forall\, g \in G$ □.

Définition : $H < G$ est distingué si

$gHg^{-1} \subset H \quad \forall\, g \in G$. Dans ce cas,

On écrit $H \lhd G$.

Non-exemple : $\langle S \rangle$ n'est pas distingué dans $\mathcal{D}_n$, car

$$\mathcal{D}_n/\langle S \rangle = \{\{I, S\}, \{R, RS\}, \dots, \{R^{n-1}, R^{n-1}S\}\}$$

$$\langle S \rangle \qquad R\langle S \rangle \qquad R^{n-1}\langle S \rangle$$

$$\langle S \rangle^{\mathcal{D}_n} = \{\{I, S\}, \{R, R^{n-1}S\}, \dots, \{R^{n-1}, RS\}\}$$

$\langle S \rangle$ $\quad$ $\langle S \rangle R$ $\quad$ $\langle S \rangle R^{n-1}$

Lemme : $f : G \longrightarrow G'$ morphisme de groupes

$\Rightarrow \operatorname{Ker} f \trianglelefteq G$.

Preuve : $\forall\, x \in \operatorname{Ker} f$, $g \in G$.

$$f(gxg^{-1}) = f(g) f(x) f(g)^{-1} = f(g) f(g)^{-1} = e'$$

$\Rightarrow gxg^{-1} \in \operatorname{Ker} f$ $\square$.

Exemple : 1. G abélien $\Rightarrow$ tout sous-groupe de G est distingué.

2. $SL_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$ car

$\{ A \in GL_n(\mathbb{K}) \mid \det A = 1 \}$

$\|$

$\operatorname{Ker} \det$

avec $\det : GL_n(\mathbb{K}) \longrightarrow \mathbb{K}^\times$.

3. $[G : H] = 2 \Rightarrow H \trianglelefteq G$.

En effet $|G/H| = |H \backslash G| = 2$.

et $eH = He$

$\Rightarrow G/H = \{ H, G - H \} = H\backslash G$.

4. $\varepsilon_{gn} : \mathfrak{S}_n \longrightarrow \mu_2 = \{1, -1\}$.

$\mathcal{A}_n = \ker \varepsilon_{gn}$ groupe alterné.

$\Rightarrow \mathcal{A}_n \triangleleft \mathfrak{S}_n$.

But : munir G/H d'une structure "naturelle" de groupe quand $H \triangleleft G$.

Idée : $\forall x, y \in G$

$xH \cdot yH = xyH$ *

Mais $xH = xhH \quad \forall h \in H$

$yH = ykH \quad \forall k \in H$

Lemme : Si $H \triangleleft G$ alors

$xyH = xhykH \quad \forall x, y \in G, \; h, k \in H$.

Preuve : $H \triangleleft G \Rightarrow$

$xhykH = xy(y^{-1}hy)kH = xyH$ □

$\in H \quad \in H$

car $y^{-1}hy \in H$.

telle que

$\pi : G \longrightarrow G/H$

morphisme de groupe.

Théorème : $H \triangleleft G$

1. G/H est un groupe avec l'opération déf, par (*), avec

eH comme élém. neutre et $(xH)^{-1} = x^{-1}H \quad \forall x \in G$.

2. $\pi : G \longrightarrow G/H$ morphisme de groupes surjectif,
$x \longmapsto xH$

$\ker \pi = H$. $\twoheadrightarrow$ surjectif.

Théorème : $f : G \longrightarrow G'$ morphisme de groupes

$\Rightarrow \bar{f} : G/\ker f \longrightarrow \operatorname{im} f$ isomorphisme.

Preuve : $K = \ker f$, $H = \operatorname{im} f$

$\bar{f} : G/K \longrightarrow H$

$xK \longmapsto f(x)$.

diagramme.

$$\begin{array}{ccc} G & \xrightarrow{f} & G \\ \pi \downarrow & & \uparrow i \leftarrow \text{injectif} \\ G/K & \xrightarrow[\bar{f}]{} & H \end{array}$$

Remarque : $G \curvearrowright X$, $K \lhd G$.

si $k \cdot x = x \quad \forall k \in K, \ x \in X$.

alors $K \subset \ker f$ pour $f : G \longrightarrow \mathfrak{S}_X$

$\Rightarrow \bar{f} : G/K \longrightarrow \mathfrak{S}_X$ définit une action

$G/K \curvearrowright X$ où $gK \cdot x = g \cdot x \quad \forall g \in G, \ x \in X$

Exemple : $\mathbb{K}^\times I_n = \{ d I_n \mid d \in \mathbb{K}^\times \} \triangleleft GL_n(\mathbb{K})$.

$\mathbb{K}^\times I_n = Z[GL_n(\mathbb{K})]$

$PGL_n(\mathbb{K}) := GL_n(\mathbb{K}) / \mathbb{K}^\times I_n$ groupe projectif général linéaire.

$\mathbb{K}^\times I_n \cap SL_n(\mathbb{K}) \triangleleft SL_n(\mathbb{K})$.

$\mathbb{K}^\times I_n \cap SL_n(\mathbb{K}) = Z[SL_n(\mathbb{K})]$

$PSL_n(\mathbb{K}) := SL_n(\mathbb{K}) / \mathbb{K}^\times I_n \cap SL_n(\mathbb{K})$ groupe projectif général linéaire.

Preuve du théorème.

$K = \ker f$, $H = \operatorname{im} f$.

$f(k) = e \quad \forall k \in K \Rightarrow f$ constante sur les orbites de l'action par translation à droite K sur G.

$\Rightarrow \bar{f} : G/K \longrightarrow H$ bien définie

$gK \longmapsto f(g)$

- $\bar{f}(gK\,hK) = \bar{f}(ghK) = f(gh) = f(g) f(h)$

$= \bar{f}(gK)\ \bar{f}(hK)$

$\Rightarrow$ $\bar{f}$ homomorphisme.

- $\ker \bar{f} = \{ gK \mid f(g) = e \} = \{ eK \}$

$\Rightarrow$ $\bar{f}$ injectif.

- $\operatorname{im} \bar{f}$ $\qquad$ $\operatorname{im} f = H$

$\{ \bar{f}(gK) \mid gK \in G/K \} = \{ f(g) \mid g \in G \}$

$\Downarrow$

$\bar{f}$ surjectif $\square$

Exemple : (i) $\mathfrak{S}_n / \mathcal{A}_n \cong \mu_2$ car

$\mathcal{A}_n = \ker \operatorname{sgn}$

$\mu_2 = \operatorname{im} \operatorname{sgn}$

avec $\operatorname{sgn} : \mathfrak{S}_n \longrightarrow \mu_2$.

(ii) $GL_n(\mathbb{K}) / SL_n(\mathbb{K}) \cong \mathbb{K}^\times$. car

$SL_n(\mathbb{K}) = \ker \det$

$\mathbb{K}^\times = \operatorname{im} \det$

avec $\det : GL_n(\mathbb{K}) \longrightarrow \mathbb{K}^\times$

$$R = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

(iii) $\det : D_n \longrightarrow \mu_2$ morphisme de groupes surjectif de noyau .

$R = \langle R \rangle \Rightarrow D_n/R \cong \mu_2$.

(iv) $S^1 = \{ z \in \mathbb{C}^* \mid |z| = 1 \}$.

$$-^n : S^1 \longrightarrow S^1, \quad z \longmapsto z^n .$$

$\ker(-^n) = \mu_n$

$\operatorname{im}(-^n) = S^1$

$\Rightarrow S^1/\mu_n \cong S^1$.

Théorème : $K \triangleleft G$, $\pi : G \longrightarrow \bar{G} = G/K$ projection canonique . ($K = \ker \pi$)

(i) $H \triangleleft G \Rightarrow \pi(H) < \bar{G}$ est isomorphe à $H/(H \cap K)$

$H \triangleleft G \Rightarrow \pi(H) \triangleleft \bar{G}$

(ii) $\bar{H} < \bar{G} \Rightarrow \pi^{-1}(\bar{H}) < G$ est le seul $K < H < G$

telque $\pi(H) = \bar{H}$.

$\bar{H} \lhd \bar{G} \Rightarrow \pi^{-1}(\bar{H}) \lhd G$

(iii) L'ensemble des sous-groupes de G contenants K est en bijection avec l'ensemble des sous-groupes de $\bar{G}$.

$$\{ H \mid K < H < G \} \longleftrightarrow \{ \bar{H} \mid \bar{H} < \bar{G} \}$$

$$H \longmapsto \pi(H)$$

Remarque : (iii) Conséquence directe de (i) et (ii)

Preuve : (i) $H / \mathrm{Ker}(\pi_{|H}) \cong \mathrm{im}(\pi_{|H})$.

$\mathrm{Ker}(\pi_{|H}) = H \cap K$, $\mathrm{im}(\pi_{|H}) = \pi(H)$.

si $H \lhd G$, $\forall \bar{g} \in \bar{G}$, $\pi(h) \in \pi(H)$.

Soit $g \in G$ tel que $\pi(g) = \bar{g}$

$\Rightarrow \bar{g}\,\pi(h)\,\bar{g}^{-1} = \pi(g)\pi(h)\pi(g)^{-1} = \pi(ghg^{-1}) \in \pi(H)$.

(ii) Soit $K < H < G$: $\pi(H) = \bar{H}$.

- $h \in H \Rightarrow \pi(h) \in \bar{H}$

  $\Rightarrow h \in \pi^{-1}(\bar{H})$

  $\Rightarrow H < \pi^{-1}(\bar{H})$.

Un groupe contenu dans un autre groupe est un sous-groupe.

- $g \in \pi^{-1}(\bar{H}) \Rightarrow \exists\, h \in H : \pi(g) = \pi(h)$.

$\Rightarrow g h^{-1} \in \ker \pi = K$

$\Rightarrow g = g h^{-1} h \in H$.

$\Rightarrow \pi^{-1}(\bar{H}) < H$.

si $\bar{H} \triangleleft \bar{G} \Rightarrow \forall\, g \in G,\ h \in \pi^{-1}(\bar{H})$.

$\pi(g h g^{-1}) = \pi(g)\,\pi(h)\,\pi(g^{-1}) \in \bar{H}$.

$\Rightarrow g h g^{-1} \in \pi^{-1}(\bar{H})$ □.

Exo 1 :

G groupe.

$$G = \left\{ \begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \;/\; a,b,c \in \mathbb{K},\ abc = 1 \right\} < Gl_3(\mathbb{K})$$

$G = K \rtimes H$?

Prendre

$$K = \left\{ \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;/\; d \in \mathbb{K} \right\}$$

$$H = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1/ab \end{pmatrix} \;/\; a,b \in \mathbb{K}^\times \right\}$$

- $K < G$:

  - $id \in K$ ok

  - $\begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & d' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & d+d' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

  - $\begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & -d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$K \lhd G$:

soit $g = \begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \in G$ fixé et

$\forall \quad x \in K$

$$\text{i.e. } x = \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{on a :}$$

$$gxg^{-1} = \begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}^{-1}$$

$\in K$ donc $K \trianglelefteq G$.

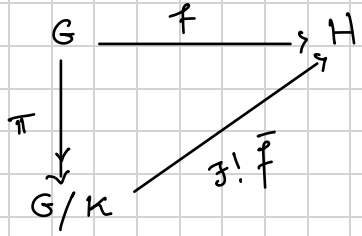
Preuve alternative : $K = \ker f$.

où $f : G \longrightarrow H$ homomorphisme

$$g \longmapsto h$$

$$\begin{pmatrix} a & 0 & d \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \qquad \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$$

$\Downarrow$ par théorème d'isomorphisme.



$f^{-1} = \pi|_H$ car $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \begin{pmatrix} 1 & 0 & d/a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\in H$ $\in K$

Exo 2 : $\langle \cdot , \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$

i) $\forall A \in \mathcal{O}_n$, $\forall x, y \in \mathbb{R}^n$.

$\langle Ax, Ay \rangle = \langle x, y \rangle \quad \forall x, y$

$\Leftrightarrow x^T A^T A y = x^T y \quad \forall x, y$

$\Leftrightarrow A^T A = Id$

$\Leftrightarrow A^T = A^{-1}$

$\Leftrightarrow \det A = \frac{1}{\det A}$

$\Leftrightarrow |\det(A)| = 1$

$\Leftrightarrow (\det(A))^2 = 1$

$\left((A^T A)_{ij} = e_i^T A^T A e_j = e_i^T e_j = \delta_{ij} \right)$

ii) Montrons que $\mathcal{O}_n = SO_n \rtimes H$.

avec $H = \left\{ \begin{pmatrix} (-1)^k & & 0 \\ & 1 & \\ 0 & & \ddots \end{pmatrix} \quad k \in \mathbb{N} \right\}$

$\mathcal{O}_n$ a bien :

$SO_n \trianglelefteq \mathcal{O}_n$ car

pour $A \in SO_n$ et $B \in \mathcal{O}_n$

On a $\det(BAB^{-1})$

$\|$

$\det(B)\det(A)\det(B^{-1})$

$\|$

1.

donc $BAB^{-1} \in SO_n$

- On a $H \cap SO_n = Id$ car

la seule matrice de det $= 1$ dans H est Id

- $H < O_n$ ok
- $O_n \xrightarrow{\pi} O_n/SO_n$ proj cano

Mq : $\pi|_H$ est un iso

$$\pi|_H = \pi(H) = \left\{ \begin{pmatrix} (-1)^k & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix} SO_n , SO_n \right\}$$

et

$\det : O_n \longrightarrow \mu_2$

$\|$?

$$\underbrace{\left\{ Id , \begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix} \right\}}_{\| \; H}$$

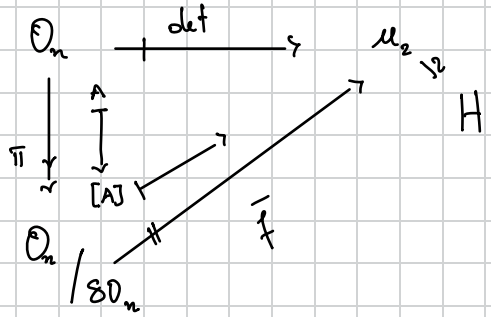
$\ker(\det \circ f) = SO_n$

$\det f$ surjective, $\mathrm{Im}(\det \circ f) = \{\pm 1\}$

donc $O_n = K \times H = SO_n \times H$

$H \cong \mu_2$.

iii)



$\pi|_H$ isométrique $\Leftrightarrow$ $\det|_H$ iso

$[I] = 1$.

$$\begin{bmatrix} -1 & & 0 \\ & 1 & \\ 0 & & 1 \end{bmatrix} = -1$$

$A \in O_n$

$$\begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}$$

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

si $A \in O_n \setminus SO_n$

A s'écrit comme le produit

$$A = \underbrace{A \begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}}_{SO_n} \begin{pmatrix} -1 & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}$$

$$SO_n \times H \xrightarrow{f} O_n$$

$$(A, h) \longmapsto Ah$$

$$f((A,h)(A',h')) = f(AA', hh') = AA'hh'$$

$$f(A,h) f(A',h') \quad \text{marche pas}$$

O_n considéré si n impaire

$$H' = \{ I_n , -I_n \}$$

$$H' \cap SO_n = \{ I_n \}$$

En général c'est faux, $\det(-I_n) = (-1)^n$

donc $H' \cap SO_n = \{ I_n \}$ si n impair

$K = SO_n$.

$\rightarrow K H' = O_n$

Car $\forall A \in O_n$, $\det(A) = 1$

$\Rightarrow A = \underset{\in K}{A} \underset{\in H}{I}$

$\det(A) = -1$

$\rightarrow A = \underset{\in K}{(-A)} \cdot \underset{\in H}{I_n}$

$\rightarrow O_n = SO_n \rtimes H'$

Mais

$H' \subset Z(O_n)$

$\Downarrow$

$H' \lhd O_n$

$\rightarrow Ah = hA$, $\forall h \in H'$, $A \in K$

$\Downarrow$

$O_n \simeq K \times H'$

Exo 3.

$$G = K \times H$$

$|K|$: $p > n \in \mathbb{N}$

$|H|$: p, premier

$\Big\Vert$?

$$G \simeq K \times \mu_p$$

$K \trianglelefteq G$.

si $H \trianglelefteq G \Rightarrow G = K \times H$

$|H| = p$,

$$|G| = |K \times H| = |K||H| = np$$

or $n < p$, on a : $n \wedge p = 1$.

$\Rightarrow$ H est un p-sylow.

H distingué $\Leftrightarrow$ $n_p = 1$

$\Leftrightarrow$: Tous les p-sylow sont conjugués

$n_p = 1$: H est le seul p-syl

si $g \in G$,

$$g H g^{-1} \leq G$$

$$|g H g^{-1}| = |H|$$

$$\| \quad p$$

$\Downarrow$

$g H g^{-1}$ p-sylow

$\Rightarrow g H g^{-1} = H$, $\forall g \in G$.

$\Rightarrow H \trianglelefteq G$.

$\Leftarrow$ $H \trianglelefteq G$. De plus, tous les p-sylow sont conjugués.

$\Rightarrow \{ p\text{-syl} \} = \{ H \} \Rightarrow n_p = 1$.

Rmq : $G = K \times H \Rightarrow |G| = |K||H|$

[$G = K \times H \Rightarrow$

en tant qu'ensemble : $G = K \cdot H$ et

$K \cap H = \{e\}$. $|K \cdot H| = \dfrac{|K||H|}{|K \cap H|} = \dfrac{|K||H|}{1}$]

$n_p \mid n$ et

$n_p \equiv 1 \pmod p \Rightarrow n_p = pk + 1, \ k \in \mathbb{N}$

si $k \geq 1$ on a $n_p > n$ donc $n_p \nmid n$

Par suite $k = 0$

donc $n_p = 1$.

donc H distingué dans G

donc $G \simeq K \times H$

et vu que p premier

On a que $H \simeq \mu_p$

donc $G \simeq K \times \mu_p$.

Exo 5 :

$G = K \rtimes H$, $H \lhd G$

$K < L < G$, $H = G$.

→ $G = H \rtimes H$, donc $K \cap H = \{e\}$

Donc $K \cap (H \cap L) = \{e\}$

→ $K \lhd G$ et $L < G$, donc $K \lhd L$

→ $K \subset L$ et $H \cap L \subset L$, donc

$K \cdot (H \cap L) \subset L$

→ Soit $l \in L$. $l \in G$, donc $\exists\, k \in K, h \in H$

tq $l = kh$. On a donc $h = k^{-1} l$

Comme $K < L$ et L est un groupe, $h \in L$

donc $\forall\, l \in L$, $\exists\, k \in K$, $h \in H \cap L$, $l = kh$

donc $L \subset K \cdot (H \cap L)$

donc $L = K \rtimes (H \cap L)$.

Exo 6 .

G ← Groupe

$|G| = pq$ (p premier, q premier)

$q \not\equiv 1 \pmod p$

$p < q$.

existence : d'après le théorème de Sylow, on a bien $p \gcd(p, q) = 1$, donc on a bien existence d'au moins un p-sylow et un q-sylow de G.

unicité : toujours par le théorème de Sylow

$n_p \mid q$ et $n_p \equiv 1 \pmod p$

$\Rightarrow n_p \in \{1, q\}$

$q \not\equiv 1 \pmod p \Rightarrow n_p \neq q$ et $n_p = 1$.

$n_q \mid p \wedge n_q = 1 \pmod q$

$p < q \Rightarrow p \not\equiv 1 \pmod q \Rightarrow$

$n_q = 1$ car pas premier.

$\Downarrow$

$G \simeq P_p \times P_q$

G cyclique : $G \simeq P_p \times P_q$

$\wr$

$\mu_p \times \mu_q$

$\wr$

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

$\simeq$

$\mathbb{Z}/pq\mathbb{Z}$.

Il existe $x_p \in P_p \mid \mathrm{Ord}(x_p) = p$

(de même il existe $x_q \in P_q \mid \mathrm{ord}(x_q) = q$)

Exemple : Groupe non abélien :

$\mathfrak{S}_6$.

2×3

2 : p ; 3 : q

Exo 7 : $G \simeq \mathbb{U}_q \times_\varphi \mathbb{U}_p \quad (q \equiv 1 \pmod p)$

(ii) $n_q = |Syl_q(G)| \qquad |G| = pq$

$n_q \mid p \quad \wedge \quad n_q \equiv 1 \pmod q$

$\Downarrow$

$n_q \in \{1, p\}$

Mais $q \equiv 1 \pmod p \Rightarrow p < q$

$\Downarrow$

$n_q \neq p$

$\Downarrow$

$n_q = 1$

Donc on a un unique q-sylow Q, qui est distingué.

Soit P un p-sylow de G

$QP = \{xy \in G \mid x \in Q, y \in P\}$

$$|QP| = \frac{|Q \times P|}{|Q \cap P|} = |Q||P|$$

$|Q \cap P| = 1$, $\quad |Q||P| = qp$

Donc $G = Q \times P$.

Mais $P \simeq \mathbb{Z}_p$ et $Q \simeq \mathbb{Z}_q$

et donc

$$G \simeq \mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p \quad \text{avec}$$

$$\begin{array}{ccc} \varphi : \mathbb{Z}_p & \longrightarrow & \mathrm{Aut}(\mathbb{Z}_q) \\ \downarrow \wr & & \downarrow \wr \\ P & & Q \end{array}$$

Exos : G simple

(i) $\ker f \trianglelefteq G \Rightarrow$

soit $\ker f = \{e\}$ ($\Rightarrow f$ inj)

soit $\ker f = G$ ($\Rightarrow f$ trivial)

(ii) $63 = 3^2 \cdot 7$

$n_7 \mid 9 \quad \wedge \quad n_7 \equiv 1 \pmod 7$

$\Downarrow$ $\qquad$ $\uparrow$

$n_7 \in \{1, 9\}$ $\qquad$ Il n'y a que 1 qui satisfait $n_7 = 1 \Rightarrow$

$\exists\, P_7 \trianglelefteq G : |P_7| = 7$

$\Rightarrow G$ n'est pas simple.

(iii) $30 = 2 \cdot 3 \cdot 5$.

$n_2 \mid 15 \quad \wedge \quad n_2 \equiv 1 \pmod 2$

$\Rightarrow n_2 \in \{1, 3, 5, 15\}$

$n_3 \mid 10 \quad \wedge \quad n_3 \equiv 1 \pmod 3$

$\Rightarrow n_3 \in \{1, 10\}$

$n_5 \mid 6 \quad \wedge \quad n_5 \equiv 1 \pmod 6$

$\Rightarrow n_5 \in \{1, 6\}$.

si par l'absurde G était simple, alors en part.

On aurait $n_3 = 10$ et $n_5 = 6$

Donc dans G il y aurait $10 \cdot \underset{2}{\underbrace{(3-1)}} = 20$

élém. d'ordre 3 et $6 \cdot \underset{4}{\underbrace{(5-1)}} = 24$

élém. d'ordre 5, mais $20 + 24 > 30$

$\longrightarrow\!\leftarrow$

(ii) $36 = 2^2 \cdot 3^2$.

$n_3 \mid 4 \quad \wedge \quad n_3 \equiv 1 \pmod 3$

$\Rightarrow n_3 \in \{1, 4\}$

si par l'absurde $n_3 = 4$, alors

$$\rho : G \longrightarrow \mathfrak{S}_{Sylow_3(G)} \simeq \mathfrak{S}_4$$

Mais $|\mathfrak{S}_4| = 24 < 36$.

Donc $\rho = id$ grâce au point (i) car G est simple par hypothèse. Mais l'action triviale n'est pas transitive.

$\longrightarrow\!\leftarrow$

Exo 10 : $a, b \in \mathbb{N}$, p, q premiers

i) On suppose $p^a < q$.

G un groupe d'ordre $p^a q^b$.

d'après le théorème de Sylow on a :

$$n_p \mid q^b \quad \wedge \quad n_p \equiv 1 \pmod p$$

Comme $p^a < q$ alors $p^a < q^b$

Soit P un p-sylow de G.

$$|P| = p^a$$

$$n_p \mid q^b \Rightarrow n_p \in \{1, q^k \mid k < b\}.$$

Puisque $n_p = 1 \pmod p$ et

$q^k = 1 \pmod p$ on veut que $p \mid q^k - 1$

mais $p^a < q$, donc $p < q$, donc $p \nmid q - 1$

et donc a fortiori ne divise pas $q^k - 1 \ \forall k$.

Ainsi, le seul entier n_p qui satisfait est $n_p = 1$

Donc, il existe un unique p-sylow, qui est alors distingué, donc G n'est pas simple.

ii) On suppose que $p^a \nmid q^b$!

Soit G un groupe d'ordre $p^a q^b$

Encore une fois, soit P un p-sylow de G.

$|P| = p^a$. On sait que G agit par conjugaison sur l'ensemble des p-sylow. Cette action induit un morphisme de groupes :

$$\varphi : G \longrightarrow \mathfrak{S}_{n_p}$$

L'image de φ est un sous-groupe de $\mathfrak{S}_{n_p}$ donc d'ordre divisant $n_p ! \mid q^b !$

donc $\ker \varphi \triangleleft G$.

si G est simple $\Rightarrow$ soit $\ker \varphi = \{id\}$

soit $\ker \varphi = G$

- s'il est trivial $\Rightarrow \varphi \hookrightarrow \Rightarrow |G| < n_p !$
- mais $|G| = p^a q^b$ et par hypothèse $p^a \nmid q^b !$

donc $|G| \nmid n_p !$

Donc contradiction, donc $\ker \varphi \neq \{e\}$ et $\neq G$,

donc G n'est pas simple.

Exo 1 : $I \neq A$ un idéal

(A : anneau)

1. Soient $x, y \in A$ / $xy \in I$

$\Downarrow \leftarrow$?

$x \in I$ ou $y \in I$

$\pi : A \to A/I$ projection canonique

$a \mapsto a + I$

$\pi(xy) = I$

$\pi(x)\,\pi(y) = I$

$\Downarrow \leftarrow$ A/I intègre.

$\pi(x) = I$ ou $\pi(y) = I$

donc $x \in I$ ou $y \in I$.

$\Leftarrow$: Soit $x + I, y + I \in A/I$ /

$(x + I)(y + I) = I$

$\Downarrow$

$xy + I = I$

donc $xy \in I \Rightarrow \begin{cases} x + I = I \\ y + I = I \end{cases}$

par hyp

d'où l'intégrité.

Remarque préliminaire.

Un anneau R est un Corps

$\Updownarrow$

$I \subset R$ idéal $\Rightarrow$ $I = \{0\}$ ou $I = R$

1) Pour tout $x \in R \setminus \{0\}$, on a $(x) \neq \{0\}$

$\Rightarrow$ $(x) = R$ $\Rightarrow$ $1 \in (x)$ $\Rightarrow$ $\exists\, y \in R$

$xy = 1$

2. I maximal $\Leftrightarrow$ ($\forall$ $J \subset A$ idéal, on a

$I \subset J \Rightarrow J = I$ ou $J = A$)

$$A \xrightarrow{\ \pi\ } A/I$$

$\uparrow$ projection Canonique

I maximal $\Leftrightarrow$ A/I corps

$\Leftrightarrow$ ($\bar{J} \subset A/I$ idéal $\Rightarrow$ $\bar{J} = \{0\}$ ou $\bar{J} = A/I$)

$\Leftrightarrow$ ($\pi^{-1}(\bar{J})$ idéal $\Rightarrow$ $\pi^{-1}(\bar{J}) = \pi^{-1}(\{0\})$ ou $\pi^{-1}(\bar{J}) = \pi^{-1}(A/I)$)

$\Leftrightarrow$ ($J \subset A$ idéal tq $I \subset J \Rightarrow J = I$ ou $J = A$)

Exo 2 : $A \xrightarrow{f} B$, I

↑ un morphisme d'anneaux.

1. $I \subset B$ ip $\Rightarrow$ $f^{-1}(I)$ ip de A.

?

Soit $x, y \in A$ / $xy \in f^{-1}(I)$.

$xy \in f^{-1}(I) \iff f(xy) \in I$

$\Leftarrow$ $f(x)f(y) \in I$ (f morphisme)

$\Leftarrow$ $f(x) \in I$ ou $f(y) \in I$ (I ip de B)

$\Leftarrow$ $x \in f^{-1}(I)$ ou $y \in f^{-1}(I)$

$\Leftarrow$ $f^{-1}(I)$ est un idéal premier de A.

2. I im de B $\Rightarrow$ $f^{-1}(I)$ pas forcé. im de A.

Contre-exemple :

$A = \mathbb{Z}$, $B = \mathbb{Q}$.

$\mathbb{Z} \hookrightarrow \mathbb{Q}$

$I = \{0\} \subset \mathbb{Q}$ maximal mais $\{0\} \subset \mathbb{Z}$ n'est pas maximal.

Exo 3 : Soit $a = (a_1, \dots, a_n) \in \mathbb{K} \times \dots \times \mathbb{K}$,

$(X_1 - a_1, \dots, X_n - a_n) \subset \mathbb{K}[X_1, \dots, X_n]$

est maximal ?

$$\varepsilon_{\underline{a}} : \mathbb{K}[X_1, \dots, X_n] \longrightarrow \mathbb{K}$$

$$P(X_1, \dots, X_n) \longmapsto P(a_1, \dots, a_n)$$

But : On sait que $\varepsilon_{\underline{a}}$ est un morphisme d'anneaux

On veut montrer que $\operatorname{im} \varepsilon_{\underline{a}} = \mathbb{K}$ et $\ker \varepsilon_{\underline{a}} = I$.

Im $\varepsilon_{\underline{a}} = \mathbb{K}$: $\forall\, b \in \mathbb{K} \subset A$, $\varepsilon_{\underline{a}}(b) = b \in \operatorname{im} \varepsilon_{\underline{a}}$

$I \subset \ker \varepsilon_{\underline{a}}$: $\varepsilon_{\underline{a}}(X_i - a_i)$

$= a_i - a_i = 0$

$\Rightarrow X_i - a_i \in \ker \varepsilon_{\underline{a}}$, $\forall\, i$

$\ker \varepsilon_{\underline{a}} \subset I$: $\forall\, i$, $X_i + I = a_i + I$

parce que $X_i - a_i \in I$

$\Downarrow$

$\forall\, P \in A$, $P(X_1, \dots, X_n) + I$

$=$

$P(a_1, \dots, a_n) + I$

$\Rightarrow$ si $\varepsilon_{\underline{a}}(P) = 0$, alors

$$P(a_1, \dots, a_n) = 0$$

et $P(X_1, \dots, X_n) \in I$

Alors grâce au théorème de noyau et image, on a que

$$\begin{array}{ccc} A/_{\text{Ker } \varepsilon_{\underline{a}}} & \xrightarrow{\sim} & \text{Im } \varepsilon_{\underline{a}} \\ \| & & \| \\ A/I & & \mathbb{K} \text{ corps} \end{array}$$

$\Downarrow$

I est maximal

Exo 4 : (i) $I + J = \{ x + y \mid x \in I , y \in I \}$

idéal.

$I + J$ clos par $+$: $x, x' \in I$, $y, y' \in J$

$(x+y) + (x'+y') = (x+x') + (y+y') \in I + J$

car I, J clos par $+$.

$I + J$ absorbe. : $a \in A$, $x \in I$, $y \in J$

$a(x+y) = ax + ay \in I + J$

car I, J absorbent.

$I = I + 0 \subset I + J$ car $0 \in J$

$J = 0 + J \subset I + J$ car $0 \in I$

$\Rightarrow I \cup J \subset I + J$

$K \subset A$ idéal, $I \cup J \subset K \Rightarrow$

$I + J \subset K$

car K est un sous-groupe (additif) de A

(ii) Mq IJ est un idéal

- $0 = x \times 0$, $x \in I$, $0 \in J$ car

J idéal

- soit $z = \sum_{i=1}^{n} x_i y_i$

$t = \sum_{i=1}^{m} x_i y_i$

$z+t = \sum_{i=1}^{n} x_i y_i + \sum_{i=1}^{m} x_i y_i \in IJ$

soit $z = \sum_{i=1}^{n} x_i y_i$

$-z = \sum_{i=1}^{n} (-x_i) y_i$ et

$-x_i \in I$ car I idéal

$-z \in IJ$

Soit $z = \sum_{i=1}^{n} x_i y_i$ et $a \in A$

$za = \sum_{i=1}^{n} x_i (y_i a)$, $y_i a \in I$

car I idéal

$\Rightarrow za \in IJ$

- Mq $IJ \subset I \cap J$

soit $z \in IJ$, $z = \sum_{i=1}^{n} x_i y_i$, $y_i \in J \subset A$

par l'absorption $x_i y_i \in I$ idéal

donc $z \in I$, et pareil pour J.

Exo 8 : Soit $p > 2$ nombre premier et

$\square_p = \{ a^2 \ / \ a \in \mathbb{F}_p^\times \}$.

1. Montrons que $\{ x \ / \ x^{\frac{p-1}{2}} - 1 = 0 \} = \square_p$.

* $\supset$: si $a \in \square_p \Rightarrow \exists\, b \in \mathbb{F}_p^\times \ / \ a = b^2$

$\Rightarrow a^{\frac{p-1}{2}} = (b^{p-1})$. Par le petit thm de Fermat,

$b^{p-1} = 1$, donc $a^{\frac{p-1}{2}} = 1$. Donc a est une

racine de $X^{\frac{p-1}{2}} - 1$.

* $\subset$: Soit $a \in \mathbb{F}_p^\times \ / \ a^{\frac{p-1}{2}} = 1$. Le polynôme

$X^{\frac{p-1}{2}} - 1$ a exactement $\frac{p-1}{2}$ racines dans $\mathbb{F}_p$.

Or, $\square_p$ a $\frac{p-1}{2}$ éléments (car l'app $x \mapsto x^2$

est surjectif dans $\mathbb{F}_p^\times$).

Donc les racines sont exactement les elmts de $\square_p$.

2. $-1 \in \square_p \Leftrightarrow p \equiv 1 \pmod 4$.

* si $p \equiv 1 \pmod 4$, $\Rightarrow \frac{p-1}{2}$ est pair.

Soit $a \in \mathbb{F}_p^\times$ un générateur. $\Rightarrow a^{\frac{p-1}{2}} = -1$.

Donc $(-1)^{\frac{p-1}{2}} = 1 \Rightarrow -1 \in \square_p$.

* si $p \equiv 3 \pmod 4$ $\Rightarrow \frac{p-1}{2}$ est impair $\Rightarrow$

$(-1)^{\frac{p-1}{2}} = -1 \quad \Rightarrow \quad -1 \notin \square_p$.

3. $p \equiv 1 \pmod 4 \Rightarrow (p) \subset \mathbb{Z}[i]$ pas premier

• si $p \equiv 1 \pmod 4 \Rightarrow -1 \in \square_p \Rightarrow \exists\, a, b \in \mathbb{Z}$ /

$p = a^2 + b^2 \Rightarrow p = (a+ib)(a-ib)$ dans $\mathbb{Z}[i]$.

Donc $(p) = (a+ib)(a-ib)$.

Comme $\mathbb{Z}[i]$ est un anneau principal,

(p) n'est pas premier car il est produit de deux

idéaux non triviaux .

4. $p \equiv 3 \pmod 4 \Rightarrow (p) \subset \mathbb{Z}[i]$ est maximal.

$\mathbb{Z}[i]$ est un anneau principal euclidien, avec

la norme $N(a+ib) = a^2 + b^2$. Si $p \equiv 3 \pmod 4$

$\Rightarrow p$ n'est pas une somme de deux carrés .

donc p reste irréductible dans $\mathbb{Z}[i]$.

donc (p) est un idéal maximal.

Exo 9 : $P \in \mathbb{K}[X]$, $\deg P \in \{2, 3\}$

(i) si P admet une racine $\alpha \in \mathbb{K}$ alors

$$P = (X - \alpha) Q .$$

$\Rightarrow$ P irréductible, alors $P = QR$ avec

$\deg Q$, $\deg R > 0$

$\Rightarrow \deg Q = 1$ ou $\deg R = 1$

(ii) On a vu en Cours que

$\mathbb{F}_p[X]/(P)$ est une $\mathbb{F}_p$-algèbre de

dimension $n = \deg P$, donc il y a p^n élmt

donc

$$\left| \mathbb{F}_2(X)/(X^2 + X + 1) \right| = 2^2 = 4$$

$0 + 0 + 1 \equiv 1 \pmod 2$

$1^2 + 1 + 1 \equiv 1 \pmod 2$

$\Downarrow$

$X^2 + X + 1$

n'admet pas de racines dans $\mathbb{F}_2$.