Ex 9 TD12

Mq $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un anneau commutatif puis que tout élément non nul de $\mathbb{Q}[\sqrt{2}]$ admet un inverse pour $\times$ dans $\mathbb{Q}[\sqrt{2}]$.

Pour mq $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un anneau commutatif, on mq c'est un sous-anneau de $(\mathbb{R}, +, \times)$.

- $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ car $\forall x \in \mathbb{Q}[\sqrt{2}]$, $\exists a \in \mathbb{Q}$ $\exists b \in \mathbb{Q}$ tq $x = a + b\sqrt{2}$ donc $x \in \mathbb{R}$.

$$\left.\begin{array}{l} \text{a. Mq } \forall (x,y) \in \mathbb{Q}[\sqrt{2}]^2,\ x - y \in \mathbb{Q}[\sqrt{2}] \\ \text{b. Mq } \forall (x,y) \in \mathbb{Q}[\sqrt{2}]^2,\ x \times y \in \mathbb{Q}[\sqrt{2}] \\ \text{c. Mq } 1_{\mathbb{R}} \in \mathbb{Q}[\sqrt{2}] \end{array}\right\} \text{propriété 11 du cours}$$

a. Soient $x \in \mathbb{Q}[\sqrt{2}]$ et $y \in \mathbb{Q}[\sqrt{2}]$

$\exists (a,b) \in \mathbb{Q}^2$ tq $x = a + b\sqrt{2}$

$\exists (a',b') \in \mathbb{Q}^2$ tq $y = a' + b'\sqrt{2}$

donc $x - y = a + b\sqrt{2} - (a' + b'\sqrt{2}) = a + b\sqrt{2} - a' - b'\sqrt{2} = (a - a') + (b - b')\sqrt{2}$
$= A + B\sqrt{2}$

avec $A = a - a' \in \mathbb{Q}$ et $B = b - b' \in \mathbb{Q}$.

Donc $x - y \in \mathbb{Q}[\sqrt{2}]$

b. Avec les mêmes notations qu'au a. :

$x \times y = (a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = aa' + ab'\sqrt{2} + ba'\sqrt{2} + bb'\sqrt{2}^2$

$= (aa' + 2bb') + (ab' + ba')\sqrt{2} = A' + B'\sqrt{2}$

avec $A' = aa' + 2bb' \in \mathbb{Q}$ et $B' = ab' + ba' \in \mathbb{Q}$

Donc $x \times y \in \mathbb{Q}[\sqrt{2}]$

c. $1_{\mathbb{R}} = 1_{\mathbb{R}} + 0_{\mathbb{R}}\sqrt{2} = A + B\sqrt{2}$ avec $A = 1_{\mathbb{R}} \in \mathbb{Q}$ et $B = 0_{\mathbb{R}} \in \mathbb{Q}$

donc $1_{\mathbb{R}} \in \mathbb{Q}[\sqrt{2}]$

Donc $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

De plus avec les mêmes notations qu'au a. :

$$\left.\begin{array}{l} x \times y = (aa' + 2bb') + (ab' + ba')\sqrt{2} \\ y \times x = (a'a + 2b'b) + (a'b + b'a)\sqrt{2} \\ = (aa' + 2bb') + (b'a + a'b)\sqrt{2} \end{array}\right\} \Rightarrow x \times y = y \times x$$

Donc $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un anneau commutatif.

Soit $x \in \mathbb{Q}[\sqrt{2}]^*$ mq x est inversible

$\exists (a,b) \in \mathbb{Q}^2$ tq $x = a + b\sqrt{2}$. Comme $x \in \mathbb{Q}[\sqrt{2}]^* \subset \mathbb{R}^*$, x admet un inverse noté x^{-1} pour $\times$ dans $\mathbb{R}$

Mq $x^{-1} \in \mathbb{Q}[\sqrt{2}]$

$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

Rq : $a^2 - 2b^2 \neq 0$

Par l'absurde : si $a^2 - 2b^2 = 0$ alors $a^2 = 2b^2$ donc $\begin{cases} 2 = \frac{a^2}{b^2} \\ b \neq 0 \text{ car si } b = 0 \text{ alors } a = 0 \text{ et } a + b\sqrt{2} = 0 \end{cases}$ donc $\sqrt{2} = \sqrt{\frac{a^2}{b^2}} = \frac{|a|}{|b|} \in \mathbb{Q}$ absurde !

donc $x^{-1} = A'' + B''\sqrt{2}$ avec $A'' = \frac{a}{a^2 - 2b^2} \in \mathbb{Q}$ et $B'' = \frac{-b}{a^2 - 2b^2} \in \mathbb{Q}$

Donc x admet un inverse pour $\times$ dans $\mathbb{Q}[\sqrt{2}]$

Concl : $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un corps.

Ex 5 TD12

① $(C,*)$ est un sous-groupe de $(G,*)$

ssi • $C \neq \emptyset$

• $\forall (x,y) \in C^2,\ x*y^{-1} \in C$

• $C \neq \emptyset$ car $e \in C$

en effet les éléments de C sont les éléments a de G qui commutent avec tous les éléments de G.

or e est un élément de G qui commute avec tous les éléments de G : $\forall x \in G,\ e*x = x*e$.

Donc $e \in C$ et $C \neq \emptyset$

• Soient $c \in C$ et $c' \in C$ alors $\forall x \in G,\ c*x = x*c$

$\forall x \in G,\ c'*x = x*c'$

mq $c*c'^{-1} \in C$.

Pour cela on prend un x quelconque dans G :

soit $x \in G$ et on mq $(c*c'^{-1})*x = x*(c*c'^{-1})$

$$\underline{(c*c'^{-1})*x} \overset{*\text{ assoc dans } G}{=} c*(c'^{-1}*x) = c*(x^{-1}*c')^{-1}$$

en effet $(x^{-1}*c')^{-1} = c'^{-1}*(x^{-1})^{-1} = c'^{-1}*x$

donc $(c*c'^{-1})*x = c*(x^{-1}*c')^{-1} = c*(c'*x^{-1})^{-1}$

$x^{-1}*c' = c'*x^{-1}$ car $c' \in C$ et $x^{-1} \in G$ donc c' commute avec x^{-1}

or $(c'*x^{-1})^{-1} = (x^{-1})^{-1}*c'^{-1} = x*c'^{-1}$

donc $(c*c'^{-1})*x = c*(x*c'^{-1}) = (c*x)*c'^{-1}$

$*$ assoc dans G

$= (x*c)*c'^{-1}$ car $c*x = x*c$ puisque $c \in C$ et $x \in G$

$= \underline{x*(c*c'^{-1})}$.

Donc $(c*c'^{-1})$ commute avec tout élément x de G

Concl : $(C,*)$ sous-gpe de $(G,*)$.

Ex 15 TD12

① Voir exercice 5-1

② Soit $(x,y) \in G^2$

$\varphi_a(x)\varphi_a(y) = (axa^{-1})(aya^{-1})$
$= ax(a^{-1}a)ya^{-1} = axya^{-1} = \varphi_a(xy)$

Donc φ_a est un morphisme du groupe $(G,\cdot)$ vers lui-même. C'est donc un endomorphisme.
Mq φ_a est bijective.

Soit $y \in G$ mq l'équation $\varphi_a(x)=y$ admet une unique solution dans G.

$\varphi_a(x)=y \Rightarrow axa^{-1}=y \Rightarrow a^{-1}(axa^{-1})a = a^{-1}ya \Rightarrow (a^{-1}a)x(a^{-1}a)=a^{-1}ya$
$\Rightarrow x = a^{-1}ya.$

Réciproquement $\varphi_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = y$ donc on peut affirmer que $\varphi_a(x)=y \Leftrightarrow x = a^{-1}ya.$

Donc $\forall y \in G\ \exists! x \in G$ tq $\varphi_a(x)=y$

Donc φ_a est une bijection de G sur G.
φ_a est un automorphisme du groupe $(G,\cdot)$.

③ en fait $B(G) = S_G$ (notations du cours)

Soit $(a,b) \in G^2$ et $x \in G$

$\varphi_a \circ \varphi_b(x) = \varphi_a(bxb^{-1}) = a(bxb^{-1})a^{-1}$
$= (ab)x(b^{-1}a^{-1}) = (ab)x(ab)^{-1} = \varphi_{ab}(x)$

Ce qui prouve que $\varphi_a \circ \varphi_b = \varphi_{ab}$ soit $\theta(a)\circ\theta(b) = \theta(ab)$

θ est un morphisme de groupes de $(G,\cdot)$ dans $(B(G),\circ)$.

L'élément neutre du groupe $(B(G),\circ)$ est id_G

et $\mathrm{Ker}(\theta) = \{a \in G \,/\, \theta(a) = id_G\}$

$a \in \mathrm{Ker}(\theta)$ ssi $\theta(a) = id_G \Leftrightarrow \varphi_a = id_G$

ssi $\forall x \in G,\ axa^{-1} = x$. Mq $\mathrm{Ker}(\theta) = \mathcal{C}$

Si $a \in \mathrm{Ker}\,\theta$ $\forall x \in G$ $(axa^{-1})a = xa \Rightarrow ax(a^{-1}a) = xa$
$\Rightarrow ax = xa.$

alors $a \in \mathcal{C}$ donc $\mathrm{Ker}\,\theta \subset \mathcal{C}$.

Réciproquement si $a \in \mathcal{C}$, $\forall x \in G$ $\varphi_a(x) = (ax)a^{-1} = (xa)a^{-1} = x$

Donc $\varphi_a = id_G$ et $a \in \mathrm{Ker}\,\theta$ donc $\mathcal{C} \subset \mathrm{Ker}\,\theta$

Concl: $\mathrm{Ker}\,\theta = \mathcal{C}$

② Ex 5 TD12 suite

Soit $a \in G$. a possède un symétrique pour $*$ dans G, que l'on note a^{-1}

Soit $b \in C$. $a * b = b * a$ car $b \in C$ donc b commute avec tous les éléments de G

$$a * b * a^{-1} = (a * b) * a^{-1} = (b * a) * a^{-1}$$

$$= b * (a * a^{-1})$$ $*$ associative dans G

$$= b * e = b$$ où e est le neutre pour $*$ dans G