Série II

Anneau et Corps

Rappel: On dit que $(A, +, \times)$ est un anneau ($+, *$ sont deux lois de composition interne sur A) si:

- $(A, +)$ est un groupe abélien
- $(A, \times)$ est un monoïde
- Distributivité de la loi $\times$ par rapport à la loi $+$ si $(x, y, z) \in A$

$$x \times (y + z) = x \times y + x \times z$$

Exercice I:

Soient A_1 et A_2 deux anneaux. On munit le produit cartésien $A_1 \times A_2$ des deux lois suivantes: $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$ et

$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$.

1) Montrer que $A_1 \times A_2$ muni de ces deux lois est un anneau. Cet anneau est appelé l'anneau produit de A_1 et A_2.

2) Montrer que $A_1 \times A_2$ est commutatif si et seulement si A_1 et A_2 sont commutatifs.

Corrigé:

1) $(A_1 \times A_2, +)$ est un groupe abélien

- associativité de $+$

Soient $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in A_1 \times A_2$

$$\begin{aligned}\Big[(a_1, a_2) + (b_1, b_2)\Big] + (c_1, c_2) &= (a_1 + b_1, a_2 + b_2) + (c_1, c_2) \\ &= (a_1 + b_1 + c_1, a_2 + b_2 c_2) \\ &= (a_1, a_2) + (b_1 + c_1, b_2 + c_2) \\ &= (a_1, a_2) + \big[(b_1, b_2) + (c_1, c_2)\big]\end{aligned}$$

- Commutativité de $+$

$$\begin{aligned}(a_1, b_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2) \\ &= (b_1 + a_1, b_2, a_2) \\ &= (b_1, b_2) + (a_1, a_2)\end{aligned}$$

l'élément neutre

$$(a_1, a_2) = (a_1 + 0_{A_1}, a_2 + 0_{A_2})$$
$$= (a_1, a_2) + (0_{A_1}, 0_{A_2})$$

donc $(0_{A_1}, 0_{A_2})$ est l'élément neutre pour + dans $A_1 \times A_2$ avec 0_{A_i} est est l'élément neutre dans A_i pour +

l'élément inverse

on a : $a_1 + (-a_1) = a_1 - a_1 = 0_{A_1}$
$a_2 + (-a_2) = a_2 - a_2 = 0_{A_2}$

$$(a_1 - a_1, a_2 - a_2) = (a_1 + (-a_1), a_2 + (-a_2))$$
$$= (a_1, a_2) + (-a_1, -a_2)$$
$$= (0_{A_1}, 0_{A_2})$$

d'où $(-a_1, -a_2)$ est l'élément symétrique de (a_1, a_2) dans $A_1 \times A_2$

donc $A_1 \times A_2$ est un groupe abélien

2) $(A_1 \times A_2, \times)$ est monoïde ?

- associativité de la loi $\times$

$$[(a_1, a_2) \times (b_1, b_2)] \times (c_1, c_2) = (a_1 b_1, a_2 b_2) \times (c_1, c_2)$$
$$= (a_1 b_1 c_1, a_2 b_2 c_2)$$
$$= (a_1, a_2)(b_1 c_1, b_2 c_2)$$
$$= (a_1, a_2)[(b_1, b_2) \times (c_1, c_2)]$$

car $\times$ est associative dans A_1 et dans A_2

- l'élément neutre pour $\times$

$$(a_1, a_2) = (a_1 e_1, a_2 e_2)$$
$$= (a_1, a_2)(e_1, e_2)$$

donc (e_1, e_2) est l'élément neutre pour $\times$ dans $A_1 \times A_2$ avec e_1 est l'élément neutre dans A_1 et e_2 dans A_2

donc $(A_1 \times A_2, \times)$ est un monoïde

- Distributivité de $\times$ par rapport à +

$$(a_1, a_2) \times [(b_1, b_2) + (c_1, c_2)] = (a_1, a_2) \times (b_1 + c_1, b_2 + c_2)$$
$$= (a_1 \times (b_1 + c_1), a_2 \times (b_2 + c_2))$$
$$= (a_1 b_1 + a_1 c_1, a_2 b_2 + a_2 c_2)$$
$$= (a_1 b_1, a_2 b_2) + (a_1 c_1, a_2 c_2)$$
$$= (a_1, a_2) \times (b_1, b_2) + (a_1, a_2) \times (c_1, c_2)$$

donc $\times$ est distributive par rapport à +

C/c $(A_1 \times A_2, +, \times)$ est un anneau

Rappel : l'anneau $(A, +, \times)$ est commutatif si la loi $\times$ est commutative

$A_1 \times A_2$ est commutatif $\Rightarrow \forall (a_1, a_2), (b_1, b_2) \in A_1 \times A_2$

$\Rightarrow (a_1, a_2)(b_1, b_2) = (b_1, b_2)(a_1, a_2)$

$\Rightarrow (a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2)$

$\Rightarrow \begin{cases} a_1 b_1 = b_1 a_1 \\ a_2 b_2 = b_2 a_2 \end{cases}$

$\Rightarrow A_1$ et A_2 sont commutatifs.

Exercice II

Pour un nombre premier $p \in \mathbb{N}$, on pose $\mathbb{Z}_p = \left\{ \frac{a}{b} / a \in \mathbb{Z}, b \in \mathbb{N}^* \text{ et } p \text{ ne divise pas } b \right\}$

1) Montrer que $\mathbb{Z}_p$ est un sous anneau de $\mathbb{Q}$

2) Montrer que, pour tout élément $x \in \mathbb{N}^*$, on a soit $x \in \mathbb{Z}_p$, soit $x^{-1} \in \mathbb{Z}_p$

3) Montrer que $U_p = \left\{ \frac{a}{b} / a \in \mathbb{Z}, b \in \mathbb{N}^* \text{ et } p \text{ ne divise ni } a \text{ ni } b \right\}$ où U_p désigne l'ensemble des éléments inversibles de $\mathbb{Z}_p$

Corrigé :

Rappel : $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$:

i) $(\mathbb{Z}_p, +)$ est un sous-groupe de $(\mathbb{Q}, +)$

ii) $\mathbb{Z}_p$ est stable pour $\times$

iii) $1_{\mathbb{Q}} \in \mathbb{Z}_p$

1) Montrons que $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$

i) $\mathbb{Z}_p \neq \emptyset$ car $0 = \frac{0}{b} \in \mathbb{Z}_p$ avec p ne divise pas b

soient $(x, y) \in \mathbb{Z}_p$

$x = \frac{a}{b}$ et $y = \frac{a'}{b'}$ avec $a, a' \in \mathbb{Z}$ et $b, b' \in \mathbb{N}^*$

$x - y = \frac{a}{b} - \frac{a'}{b'} = \frac{ab' - a'b}{bb'} \in \mathbb{Z}_p$ car $ab' - a'b \in \mathbb{Z}$ et $bb' \in \mathbb{N}^*$

Il ne reste que montrer que p ne divise pas bb'

si p / bb' et puisque p est premier alors p / b ou p / b' $\Rightarrow$ absurde

donc p ne divise pas bb'

par suite $(\mathbb{Z}_p, +)$ est un sous-groupe de $(A, +)$

i i) Montrons que $\mathbb{Z}_p$ est stable pour la loi $\times$

soient $x = \frac{a}{b}$ et $y = \frac{a'}{b'} \in \mathbb{Z}_p$ avec $(a$ et $a' \in \mathbb{Z})$ et $(b, b' \in \mathbb{N}^*)$

$x \times y = \frac{aa'}{bb'}$ on a $aa' \in \mathbb{Z}$ et $bb' \in \mathbb{N}^*$

et p ne divise pas bb'

donc $x \times y \in \mathbb{Z}_p$ alors $\mathbb{Z}_p$ est stable pour la loi $\times$

i i i) $1_{\mathbb{Q}} = 1 = \frac{p+1}{p+1} \in \mathbb{Z}_p$ car $p+1 \in \mathbb{Z}$ et $p+1 \in \mathbb{N}^*$ et $p \nmid p+1$

donc $\mathbb{Z}_p$ est un sous anneau de $\mathbb{Q}$

2) on montre que pour tout $x \in \mathbb{Q}^*$ $x = \frac{a}{b}$ / $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$

si $p \nmid b \Rightarrow x \in \mathbb{Z}_p$

si $p / b \Rightarrow p \nmid a$ car $(a \wedge b = 1)$

$\Rightarrow x^{-1} = \frac{b}{a} \in \mathbb{Z}_p$

3) soit $E = \left\{ \frac{a}{b} / a \in \mathbb{Z}^* \text{ et } b \in \mathbb{N}^* \text{ et } p \nmid a \text{ et } p \nmid b \right\}$

Montrons que $E = U_p$ ($A \subset B$ et $B \subset A \Leftrightarrow A = B$)

$U_p = \left\{ x \in \mathbb{Z}_p \text{ et } x^{-1} \in \mathbb{Z}_p \right\}$

$x \in U_p \Leftrightarrow x \in \mathbb{Z}_p$ et $x^{-1} \in \mathbb{Z}_p$

$\Leftrightarrow x = \frac{a}{b}$, $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$ et $p \nmid b$

et $x^{-1} = \frac{b}{a}$, $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}^*$ et $p \nmid a$

$\Leftrightarrow x \in E$

alors $E = U_p$

Exercice III :

Soient A un anneau commutatif. on pose $B = A \times A$. on munit B des lois suivantes : Pour tout $(x, e), (y, f) \in A$??, $(x, e) + (y, f) = (x+y, e+f)$

et $(x, e)(y, f) = (xy, xf + ye)$

1) Montrez que B est un anneau commutatif

2) Montrez que B n'est pas intègres

3) Déterminer l'ensemble des éléments inversibles de B.

4) on pose $A = \mathbb{Z}/2\mathbb{Z}$ montrer que, bien que B est de cardinal 4, il n'est pas isomorphe à l'anneau produit $A \times A$.

Corrigé.

1) a) Montrons que $(B,+)$ est un groupe abélien

• associativité :

Soient $(x,e),(y,f),(z,g) \in B$

$$\begin{aligned}\big[(x,e)+(y,f)\big]+(z,g) &= (x+y,e+f)+(z,g)\\ &= (x+y+z,e+f+g)\\ &= (x+(y+z),e+(f+g))\\ &= (x,e)+\big((y,f)+(z,g)\big)\end{aligned}$$

$+$ est associative.

• Commutativité :

$$\begin{aligned}(x,e)+(y,f) &= (x+y,e+f)\\ &= (y+x,f+e)\\ &= (y,f)+(x,e)\end{aligned}$$

donc $+$ est commutative.

• l'élément neutre

$$(x,e)+(a,b)=(x,e)$$

$$(x+a,e+b)=(x,e)$$

$$\begin{cases} x+a=x \\ e+b=e \end{cases} \Leftrightarrow \begin{cases} a=0 \\ b=0 \end{cases}$$

donc l'élément neutre de $+$ est $(0,0)$

• l'inverse

$$(x,e)+(y,f)=(0,0)$$

$$(x+y,e+f)=(0,0)$$

$$\begin{cases} x+y=0 \\ e+f=0 \end{cases} \Leftrightarrow \begin{cases} y=-x \\ f=-e \end{cases}$$

donc l'élément inverse de (x,e) est $(-x,-e)$

alors $(B,+)$ est un groupe abélien

2) a) on montre que $(B,\times)$ est un monoïde

• associativité :

Soit $(x,e),(y,f),(z,g) \in B$

$(x,e)\left[(y,f)(z,g)\right] = (x,e)(yz, yg+zf)$

$= (xyz, xyg+xzf+eyz)$

$= \cancel{(xyz+z,}$

$\left[(x,e)(y,f)\right](z,g) = (xy, xf+ye)(z,g)$

$= (xyz, xyg+xzf+yze)$

donc $(x,e)\left[(y,f)(z,g)\right] = \left[(x,e)(y,f)\right](z,g)$

donc $\times$ est associative.

- l'élément neutre

$(x,e)(a,b) = (xe)$

$(xa, xb+ae) = (x,e)$

$\begin{cases} xa = x \\ xb+ae = e \end{cases} \Leftrightarrow \begin{cases} a = 1 \\ xb+e = e \end{cases} \Leftrightarrow \begin{cases} a = 1 \\ b = 0 \end{cases}$

donc l'élément neutre de $\times$ est $(1,0)$

d'où $(B,\times)$ est monoïde

iii) distributivité de $\times$ sur $+$

$(x,e)\times\left[(y,f)+(z,g)\right] = (x,e)\times(y+z, f+g)$

$= \left(x(y+z), x(f+g)+e(y+z)\right)$

$= (xy+xz, xf+xg+ey+ez)$

$= (xy+xz, xf+ye+xg+ze)$

$= (xy, xf+ye)+(xz, xg+ze)$

$= (x,e)\times(y,f)+(x,e)\times(z,g)$

donc $\times$ est distributive sur $+$ dans B

enfin $(B,+,\times)$ est un anneau commutatif

e) B est intègre si $\forall x,y \in A$ alors si $xy = 0 \Rightarrow x = 0$ ou $y = 0$

on a $(0,1) \neq (0,0)$

$(0,1)\times(0,1) = (0,0)$

donc B n'est pas intègre.

3) soit $U(B)$ l'ensemble des éléments inversibles de B

soit $(x,e) \in U(B)$

$(x,e) \in B$ et $(x,e)^{-1} \in B$

soit $(y,f) \in B$ t.q $(x,e)(y,f) = (1,0)$

$(xy, xf+ey) = (1,0)$

$\begin{cases} xy = 1 \\ xf + ey = 0 \end{cases} \Rightarrow \begin{cases} y = x^{-1} \\ f = -ex^{-2} \end{cases}$

$U(B) = \{(x^{-1}, -ex^{-2}) \ / \ (x,y) \in B\}$

4) $A = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$

$A \times A = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},0), (\bar{1},\bar{1})\}$

$f : A \to B$; supposons que x est indépendant

isomorphisme $/ \exists n : x^n = e$

$\Leftrightarrow f(x^n) = f(e) = e'$

f homomorphisme $\Leftrightarrow [f(x)]^n = e'$

$f(x)$ est indépendant dans B

Dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ muni de la loi produit

$(\bar{0},\bar{1})(\bar{0},\bar{1}) = (\bar{0},\bar{1})$

$(\bar{1},\bar{0})(\bar{1},0) = (\bar{1},\bar{0})$

$(\bar{1},\bar{1})(\bar{1},\bar{1}) = (\bar{1},\bar{1})$

Dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ muni de la loi $*$

$(\bar{0},\bar{1})(0,\bar{1}) = (\bar{0},\bar{0})$

$(\bar{1},\bar{0})(\bar{1},\bar{0}) = (\bar{0},\bar{0})$

$(\bar{1},\bar{1})(\bar{1},\bar{1}) = (\bar{0},\bar{0})$

$(\bar{0},\bar{1})$ indépendant dans $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, *)$

supposant qu'il existe un isomorphisme

$f : (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, *) \to (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \cdot)$

$\mathbb{C} \to \mathbb{C}$

Exercice 4 (suite l'exercice 1)

On suppose que A_1 et A_2 sont commutatifs.

1) On suppose, dans cette question, que $A_1 = A_2 = A$ et on pose $\Delta = \{(x,x) / x \in A\}$

a) Montrer que Δ est un sous anneau de $A \times A$

b) Montrer que Δ est isomorphe à A

c) est ce que Δ est idéal de $A \times A$

2) (facultatif)

a) Montrer que le produit cartésien de deux idéaux des anneaux A_1 et A_2, respectivement, est un idéal de $A_1 \times A_2$

b) Que peut-on dire de la réciproque ?

Réponse :

1)

a) montrons que $(\Delta, +)$ est un sous-groupe de $(A \times A, +)$

- $(0,0) \in \Delta \Leftrightarrow \Delta \neq \emptyset$
- soient $(x,x), (y,y) \in \Delta$

$$(x,x) - (y,y) = (x-y, x-y) \in \Delta$$

donc $(\Delta, +)$ est un sous groupe de $A \times A$

- montrons que $\times$ est stable dans Δ

soient $(x,x), (y,y) \in \Delta$

$(x,x) \times (y,y) = (xx, yy) \in \Delta$ donc $\times$ est stable dans Δ

et $(1,1) \in \Delta$ donc Δ est un sous anneaux de $A \times A$

b) soient $x, y \in A$

- $\epsilon(x+y) = (x+y, x+y)$
  $= (x,x) + (y,y)$
  $= \epsilon(x) + \epsilon(y)$
- $\epsilon(1_A) = (1_A, 1_A) = 1_\Delta$

Rappel : $f : A \longrightarrow \Delta$, $x \longmapsto (x,x)$

f est un homomorphisme d'anneaux si :

1) $f(x+y) = f(x) + f(y)$
2) $f(xy) = f(x) \cdot f(y)$
3) $f(1_A) = 1_\Delta = 1_{A \times A}$

donc ϵ est un homomorphisme d'anneaux

avec ϵ est inj $\Rightarrow \epsilon$ est inj et par suite Δ est isomorphe à A.

c) on a $\forall (a,b) \in A \times A$ tel que $a \neq b$

et $\forall (x,x) \in I$ on a $(x,x)(a,b) = (xa, xb)$

donc Δ n'est pas idéal

2) (facultatif)

a) I_1 est l'idéal de A_1
I_2 est l'idéal de A_2
$I_1 \times I_2$ est l'idéal de $A_1 \times A_2$?

Soient $(x_1, x_2) \in I_1 \times I_2$
$(y_1, y_2) \in I_1 \times I_2$

$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \in I_1 \times I_2$

soient $(x_1, x_2) \in I_1 \times I_2$
$(a_1, a_2) \in A_1 \times A_2$
$(x_1, x_2) * (a_1, a_2) = (x_1 a_1, x_2 a_2) \in I_1 \times I_2$
donc $I_1 \times I_2$ est un idéal de $A_1 \times A_2$

b) supposons que $\mathcal{J}$ est un idéal de $A_1 \times A_2$
$\exists ?$ I_1 idéal de A_1
$\exists ?$ I_2 idéal de A_2 tel que $\mathcal{J} = I_1 \times I_2$

Posons : $I_1 = \{ a_1 \in A_1 \,/\, \exists\, a_2 \in A_2 : (a_1, a_2) \in \mathcal{J} \}$

$I_2 = \{ a_2 \in A_2 / \exists\, a_1 \in A_1 : (a_1, a_2) \in \mathcal{J} \}$

Montrons que I_1 est un idéal de A_1
soient a_1 et $a'_1 \in I_1 \Rightarrow \exists\, a_2$ et $a'_2 \in A_2$
tel que (a_1, a_2) et $(a'_1, a'_2) \in \mathcal{J}$

$(a_1, a_2) + (a'_1, a'_2) = (a'_1 + a_1, a_2 + a'_2) \in \mathcal{J}$
donc $a_1 + a'_1 \in I_1$
soient $x \in I_1$, $a_2 \in A_1$
$x \in I_1 \Rightarrow \exists\, y\, A_2$ tel que $(x, y) \in \mathcal{J}$

$(x, y) \cdot (a_1, 0) = (x a_1, 0) \in \mathcal{J} \Rightarrow x_1 a_1 \in \mathcal{J}$
$\in \mathcal{J}$ $\quad \in A_1 \times A_2$

de même on montre que I_2 est un idéal de A_2
Montrons que : $\mathcal{J} = I_1 \times I_2$
- $\mathcal{J} \subset I_1 \times I_2$
- $I_1 \times I_2 \subset \mathcal{J}$

soient $(x,y) \in J \Rightarrow x \in A_1$ et $y \in A_2$

donc $J \subset I_1 \times I_2$

soient $(x,y) \in I_1 \times I_2 \Rightarrow x \in I_1 \Rightarrow \exists x' \in A_2$ tq $(x,x') \in J$

$y \in I_2 \Rightarrow \exists y' \in A_2$ tel que $(y,y') \in J$

$(x,y) = (x,x')(1,0) + (y',y')(0,1) \in J$

donc $I_1 \times I_2 \subset J$ d'où $J = A_1 \times A_2$

Exercice 5 (facultatif)

Soit A un anneau commutatif non nul dont le corps ③

1) Montrer que A contient $\mathbb{Z}$

2) en déduire que tout idéal de A est principal.

Corrigé :

1) soit $k \in \mathbb{Z}$. $k \overset{?}{\in} A$

$1 \in A$

$k = k.1$

$= \underbrace{1+1\ldots+1}_{k \text{ fois}} \in A$ donc $\mathbb{Z} \subset A$

2) soit I un idéal de A

$I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$

$I \cap \mathbb{Z} = n\mathbb{Z} = nk \ / \ k \in \mathbb{Z}$

Montrons que $I = \langle n \rangle = nk$, $k \in \mathbb{Z}$

puisque $n \in I$, $\forall k \in A \Rightarrow kn \in I$

$\langle n \rangle \subset I$

soit $x \in I$, $\exists (p,q)$, $x = \frac{p}{q}$

$qx = p \in \mathbb{Z}$

$qx \in I \cap \mathbb{Z} = n\mathbb{Z}$

$qx = kn$

$x = \frac{k}{q} n$

$\frac{k}{q} = \frac{k}{q} . 1$ $\quad p \wedge q = 1 \Rightarrow \exists u,v \in \mathbb{Z}, pu + qv = 1$

$\frac{k}{q} = \frac{k}{q}(pu+qv)$

$= k\left(\frac{p}{q}u + v\right)$

$= kxv + kv \in A$

$\Rightarrow x \in \langle n \rangle$

Exercice 6 :

Soit $a \in \mathbb{Z}^+$. On pose $\mathbb{Z}[\sqrt{a}] = \{x + y\sqrt{a} \,/\, (x,y) \in \mathbb{Z}^2\}$ et

$\mathbb{Q}(\sqrt{a}) = \{x + y\sqrt{a} \,/\, (x,y) \in \mathbb{Q}^2\}$

1) (facultatif) Montrer que $\mathbb{Z}[\sqrt{a}]$ est un anneau commutatif

2) Montrer que $\mathbb{Q}[\sqrt{a}]$ est le corps des fractions de l'anneau $\mathbb{Z}[\sqrt{a}]$

3) (facultatif) Montrer que $\mathbb{Q}[\sqrt{a}]$ est le plus petit sous corps de $\mathbb{R}$, au sens de l'inclusion, contenant $\mathbb{Z}$ et $\sqrt{a}$.

Corrigé :

1) Vérifions que $\mathbb{Z}[\sqrt{a}]$ est un groupe commutatif

Soit $e, f, g \in \mathbb{Z}[a]$ donc $e = x_1 + y_1\sqrt{a}$
$f = x_2 + y_2\sqrt{a}$
$g = x_3 + y_3\sqrt{a}$

$$e + (f+g) = x_1 + y_1\sqrt{a} + (x_2 + x_3 + (y_2 + y_3)\sqrt{a})$$
$$= (x_1 + x_2 + (y_1 + y_2)\sqrt{a}) + x_3 + y_3\sqrt{a}$$
$$= (e+f) + g$$

$\Rightarrow$ $+$ est associative dans $\mathbb{Z}[\sqrt{a}]$

Soit $b \in \mathbb{Z}[\sqrt{a}]$ donc $b = x + y\sqrt{a}$

$b + e = b \Leftrightarrow e = 0$

Soit $b \in \mathbb{Z}[\sqrt{a}]$ $\exists ? c \in \mathbb{Z}[\sqrt{a}] \,/\, c + b = 0$

$b + c = 0$

$c = -b = -x - y\sqrt{a}$

donc $\mathbb{Z}[\sqrt{a}]$ est un groupe commutatif

2) M.q $\mathbb{Q}[\sqrt{a}] = \text{Frac}(\mathbb{Z}[\sqrt{a}])$

Soit $X \in \mathbb{Q}[\sqrt{a}] \Rightarrow \exists x, y \in \mathbb{Q} \,(X = x + y\sqrt{a})$

$x \in \mathbb{Q} \Rightarrow x = p/q \;;\; (p,q) \in \mathbb{Z} \times \mathbb{N}^*$

$y \in \mathbb{Q} \Rightarrow y = p'/q' \;;\; (p',q') \in \mathbb{Z} \times \mathbb{N}^*$

$$X = \frac{p}{q} + \frac{p'}{q'}\sqrt{a} = \frac{pq' + qp'\sqrt{a}}{qq' + 0\sqrt{a}} \in \mathbb{Z}[\sqrt{a}]$$
$$\in \mathbb{Z}[\sqrt{a}]$$

$\Rightarrow X \in \text{Frac}(\mathbb{Z}[\sqrt{a}])$

donc $\mathbb{Q}[\sqrt{a}] \subset \text{fsc}(\mathbb{Z}[\sqrt{a}])$

Soit $X \in \text{fsc}(\mathbb{Z}[\sqrt{a}])$

$$X = \frac{x+y\sqrt{a}}{x'+y'\sqrt{a}} = \frac{xx'-yy'a}{x'^2-y'^2a} + \frac{(yx'-xy')}{x'^2-y'^2a}\sqrt{a} \in \mathbb{Q}[\sqrt{a}]$$

$$\Rightarrow \text{fsc}(\mathbb{Z}[\sqrt{a}]) = \mathbb{Q}[\sqrt{a}]$$

d'où $\mathbb{Q}[\sqrt{a}] = \text{fsc}(\mathbb{Z}[a])$

3) Soit A un sous-corps de $\mathbb{R}$ contenant $\mathbb{Z}$ et $\sqrt{a}$

Montrons que $\mathbb{Q}[\sqrt{a}] \subset A$

Soient $X = x + y\sqrt{a} \in \mathbb{Q}[\sqrt{a}]$

$x \in \mathbb{Q} \Rightarrow \exists (p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ tq $x = p/q$

$y \in \mathbb{Q} \Rightarrow \exists (p',q') \in \mathbb{Z} \times \mathbb{Z}^*$ tq $y = p'/q'$

et $X = \frac{p}{q} + \frac{p'}{q'}\sqrt{a}$

on a $\mathbb{Z} \subset A$ et $\sqrt{a} \in A$

on a $p \in \mathbb{Z} \Rightarrow p \in A$ } et comme A est un corps alors $p/q \in A$
$q \in \mathbb{Z}^* \Rightarrow q \in A$ }

de même pour p' et q' $\Rightarrow p'/q' \in A$

d'où $X = \frac{p}{q} + \frac{p'}{q'}\sqrt{a} \in A$

par suite $\mathbb{Q}[\sqrt{a}] \subset A$ d'où $\mathbb{Q}[\sqrt{a}]$ est le plus petit sous corps contenant $\mathbb{Z}$ et $\sqrt{a}$

Exercice 7 :

Montrer que si A est un anneau commutatif de caractéristique un nombre premier p alors l'application $f : A \to A$, définie par $f(x) = x^p$ $(\forall x \in A)$ est un homomorphisme d'anneaux.

Corrigé :

$f(1) = 1^p = 1$

Soient $(x,y) \in A^2$: $f(xy) = (xy)^p = x^p y^p = f(x) f(y)$

$$f(x+y) = (x+y)^p = \sum_{k=0}^{p} C_p^k x^k y^{p-k} = x^p + \sum_{k=1}^{p-1} x^k y^{p-k} + y^p$$

Montrons que si p premier p / C_p^k

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{p}{k} C_{p-1}^{k-1} \Rightarrow \sum_{k=1}^{p-1} x^k y^{p-k} = 0$$

donc $f(x+y) = x^p + y^p = f(x) + f(y)$

par suite f est un homomorphisme des anneaux.