Corrigé du DM 2

Chapitre 2 exercice 16

1. On suppose $p \wedge a = 1$ et $p \wedge b = 1$.

D'après le théorème de Bézout,
$\exists (u_1, v_1) \in \mathbb{Z}^2$ tel que $u_1 p + v_1 a = 1$. (1)
$\exists (u_2, v_2) \in \mathbb{Z}^2$ tel que $u_2 p + v_2 b = 1$. (2)
En multipliant les équations (1) et (2), on obtient :

$$\underbrace{(u_1 u_2 p + u_1 v_2 b + u_2 v_1 a)}_{\in \mathbb{Z}} p + \underbrace{(v_1 v_2)}_{\in \mathbb{Z}} (ab) = 1.$$

Donc, d'après le théorème de Bézout, $p \wedge (ab) = 1$.

2. Soit p un nombre premier.

a) Soit $k \in [\![1, p-1]\!]$. $\left(\begin{array}{c} p \\ k \end{array} \right) = \dfrac{p!}{k!(p-k)!} = \dfrac{p(p-1)...(p-k+1)}{k!}$.

Donc $\binom{p}{k} k! = p(p-1)...(p-k+1)$.

donc $p \mid \binom{p}{k} k!$. (3)

Or, $\forall i \in [\![1, k]\!]$, $p \wedge i = 1$ (car p est premier) donc, d'après 1., $p \wedge k! = 1$.

Donc, d'après le lemme de Gauss, (3) $\Longrightarrow p \mid \binom{p}{k}$.

b) Procédons par récurrence sur n.
Pour $n = 0$ et pour $n = 1$, la propriété est vérifiée.
Soit $n \in \mathbb{N}$.
Supposons que la propriété (P_n) : $n^p \equiv n \ [p]$ soit vérifiée.

Alors, d'après la formule du binôme de Newton, $(n+1)^p = n^p + \sum_{k=1}^{p-1} \binom{p}{k} n^k + 1$. (4)

Or $\forall k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$ donc $p \mid \sum_{k=1}^{p-1} \binom{p}{k} n^k$.
Donc d'après (4) et (P_n), $(n+1)^p \equiv n+1 \ [p]$ et (P_{n+1}) est vraie.

c) Soit $n \in \mathbb{N}$ tel que p ne divise pas n.
Comme p est premier, alors $p \wedge n = 1$.
La question précédente donne p divise $n^p - n = n(n^{p-1} - 1)$.
Or comme p est premier avec n, on en déduit, d'après le lemme de Gauss, que p divise $n^{p-1} - 1$.
Ce qui signifie que $n^{p-1} \equiv 1 \ [p]$. (petit théorème de Fermat).

Chapitre 2 exercice 11

1. Soit $m \geqslant n$.

Il existe donc $k \in \mathbb{N}$ tel que : $m = k + n$, donc $x^m = x^n \times x^k$. Or $x^n \in I, x^k \in A$ et I est un idéal de A ; donc : $x^m \in I$.

Donc :

$$\boxed{\forall m \geqslant n, x^m \in I.}$$

2. Soit $x, y \in \sqrt{I}$. Il existe donc $n, m \in \mathbb{N}$ tels que $x^n \in I$ et $y^m \in I$. De plus A est un anneau commutatif, donc d'après la formule du binôme de Newton :

$$\begin{aligned}(x-y)^{n+m} &= \sum_{k=0}^{n+m} (-1)^k \binom{n+m}{k} x^k y^{m+n-k} \\ &= y^m \left(\sum_{k=0}^{n} (-1)^k \binom{n+m}{k} x^k y^{n-k} \right) \\ &\quad + x^n \left(\sum_{k=n+1}^{n+m} (-1)^k \binom{n+m}{k} x^{k-n} y^{m+n-k} \right) \\ &\in I \qquad (\text{car } x^n \in I \text{ et } y^m \in I)\end{aligned}$$

Donc I est un sous-groupe de $(A, +)$.

Soit de plus $a \in A$, comme A est commutatif, $(xa)^n = x^n a^n \in I$ car $x^n \in I$. Donc :

$$\boxed{\sqrt{I} \text{ est un idéal de } A.}$$

3. Soit J un idéal de A et $x \in J$, donc $x^1 \in J$ donc $x \in \sqrt{J}$. On a montré que pour tout idéal J de A, $J \subset \sqrt{J}$; or $\sqrt{I}$ est un idéal de A, donc $\sqrt{J} \subset \sqrt{\sqrt{I}}$.

Soit $x \in \sqrt{\sqrt{I}}$, donc il existe $n \in \mathbb{N}$ tel que $x^n \in \sqrt{I}$, donc il existe $m \in \mathbb{N}$ tel que $x^{nm} = (x^n)^m \in I$; donc $x \in \sqrt{I}$. On a montré que $\sqrt{\sqrt{I}} \subset \sqrt{I}$.

Conclusion :

$$\boxed{\text{Montrer que } \sqrt{\sqrt{I}} = \sqrt{I}.}$$

4. • Soit $x \in \sqrt{I \cap J}$, il existe donc $n \in \mathbb{N}$ tel que $x^n \in I \cap J$, donc $x^n \in I$, donc $x \in \sqrt{I}$ et de même $x \in \sqrt{J}$. Donc $x \in \sqrt{I} \cap \sqrt{J}$. On a montré que $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

• soit $x \in \sqrt{I} \cap \sqrt{J}$, donc $x \in \sqrt{I}$, donc il existe $n \in \mathbb{N}$ tel que $x^n \in I$ et de même il existe $n' \in \mathbb{N}$ tel que $x^{n'} \in J$; d'après la question 1, en posant $m = \max(n, n')$, $x^m \in I \cap J$, donc $x \in \sqrt{I \cap J}$. On a montré que $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cap J}$.

Donc :

$$\boxed{\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.}$$

- Soit $x \in \sqrt{I}$, il existe donc $n \in \mathbb{N}$ tel que $x^n \in I$; or $I \subset I+J$, donc $x^n \in (I+J)$, donc $x \in \sqrt{I+J}$. On a montré que $\sqrt{I} \subset \sqrt{I+J}$.
- De même, $\sqrt{J} \subset \sqrt{I+J}$.
- Or $\sqrt{I+J}$ est un idéal de A et $\sqrt{I}+\sqrt{J}$ est le plus petit idéal de A qui contient $\sqrt{I}$ et $\sqrt{J}$, donc :

$$\boxed{\sqrt{I}+\sqrt{J} \subset \sqrt{I+J}.}$$

5. La décomposition en nombres premiers de 3648 est : $2^6 \times 3 \times 19$. Donc pour $x \in \mathbb{Z}$:

$$\begin{aligned} x \in 3648\mathbb{Z} &\Leftrightarrow 2^6 \times 3 \times 19 \mid x \\ &\Leftrightarrow 2^6 \mid x \text{ et } 3 \mid x \text{ et } 19 \mid x \\ &\Leftrightarrow x \in 2^6\mathbb{Z} \cap 3\mathbb{Z} \cap 19\mathbb{Z} \end{aligned}$$

Donc : $3648\mathbb{Z} = 2^6\mathbb{Z} \cap 3\mathbb{Z} \cap 19\mathbb{Z}$.

Soit p un nombre premier et $n \in \mathbb{N}^*$, montrons que $\sqrt{p^n\mathbb{Z}} = p\mathbb{Z}$.

- Soit $x \in p\mathbb{Z}$, donc $x^n \in p^n\mathbb{Z}$. On a montré que : $p\mathbb{Z} \subset \sqrt{p^n\mathbb{Z}}$.
- Soit $x \in \sqrt{p^n\mathbb{Z}}$, il existe donc $k \in \mathbb{N}$ tel que $x^k \in p^n\mathbb{Z} \subset p\mathbb{Z}$. Donc $p \mid x^k$; or p est premier, donc d'après le lemme de Gauss, $p \mid x$, donc $x \in p\mathbb{Z}$. On a montré que $\sqrt{p^n\mathbb{Z}} \subset p\mathbb{Z}$.

Donc : $\sqrt{p^n\mathbb{Z}} = p\mathbb{Z}$.

Donc :

$$\begin{aligned} \sqrt{3648\mathbb{Z}} &= \sqrt{2^6\mathbb{Z} \cap 3\mathbb{Z} \cap 19\mathbb{Z}} \\ &= \sqrt{2^6\mathbb{Z}} \cap \sqrt{3\mathbb{Z}} \cap \sqrt{19\mathbb{Z}} && \text{(d'après 3)} \\ &= 2\mathbb{Z} \cap 3\mathbb{Z} \cap 19\mathbb{Z} \\ &= (2 \times 3 \times 19)\mathbb{Z} && \text{(d'après le lemme de Gauss)} \end{aligned}$$

Donc

$$\boxed{\sqrt{3648\mathbb{Z}} = 114\mathbb{Z}.}$$