

Algèbre 2^e année

Corrigé 9

1. (a) Tout d'abord, on a besoin de l'affirmation suivante :

Soit R un anneau. Alors chaque idéal $I \neq R$ est contenu dans un idéal maximal.

La preuve utilise le lemme de Zorn, qui constate :

Si (S, \leq) est un ensemble partiellement ordonné non-vide dans laquelle chaque chaîne $x_1 \leq x_2 \leq \dots$ est bornée dans S , alors il existe un élément maximal de S .

Étant donné le lemme de Zorn, on pose S l'ensemble des idéaux $J \subset R$, tels que $J \neq R$ et $I \subset J$, ordonné par l'inclusion. L'ensemble S est non-vide puisque $I \in S$. Si $J_1 \subset J_2 \subset \dots$ est une chaîne d'inclusions dans S , alors on pose $J = \cup_{r \geq 1} J_r$. On vérifie que J est bien un idéal de R : $0 \in J$ parce que $0 \in J_1$. Si $x, y \in J$ alors il existe $r > 0$ tel que $x, y \in J_r$, alors $x - y \in J_r \subset J$, donc J est un groupe abélien. Si $x \in R$ et $y \in J$, alors il existe $r > 0$ tel que $y \in J_r$, donc $xy \in J_r \subset J$, C.Q.F.D. De plus, $J \neq R$. En effet, si $1 \in J$, alors il existe $r > 0$ tel que $1 \in J_r$, alors $J_r = R$, contradiction. Par conséquent, $J \in S$ et la chaîne $J_1 \subset J_2 \subset \dots$ est bornée dans S . Par le lemme de Zorn, S possède un élément maximal, ce qui établit l'affirmation.

Supposons que R est local. On montre la contraposée, c-à-d, si x n'est pas inversible, alors $x \in M$. Si x n'est pas inversible, alors $(x) \neq R$. Donc (x) est contenu dans un idéal maximal, forcément M .

Ensuite, supposons que x est inversible si $x \notin M$. Soit M' un idéal maximal tel que $M' \neq M$. Puisque M' est maximal, $M' \not\subset M$, alors il existe $x \in M'$ tel que $x \notin M$. Par hypothèse, x est inversible, donc $M' = R$, contradiction.

- (b) Soit M l'unique idéal maximal de R . Soit $x \in R$. Si $x \notin M$, alors $x \in R^*$ par l'exercice ci-dessus. Si $x \in M$, alors $1 - x \notin M$. En effet, si $1 - x \in M$, alors $1 = x + (1 - x) \in M$ alors $M = R$, contradiction. Par conséquent, $1 - x \in R^*$ par l'exercice 1(a).

Un élément $x \in R$ est idempotent si $x^2 = x$. Alors $x(1 - x) = 0$. On sait que soit $x \in R^*$, soit $1 - x \in R^*$, et qu'un élément inversible n'est pas diviseur de zéro. Si $x \in R^*$, alors $1 - x = 0$, c-à-d $x = 1$. Si $1 - x \in R^*$, alors $x = 0$. Par conséquent, les seuls idempotents de R sont 0 et 1.

2. (a) Puisque $0 \in I$, on a $0 \in \sqrt{I}$. Si $x, y \in \sqrt{I}$, disons que $x^n \in I$ et $y^m \in I$. On constate que $(x + y)^{n+m} \in I$. En effet, par la formule du binôme,

$$(x + y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}.$$

Si $k \geq n$, alors $x^k \in I$, donc $x^k y^{n+m-k} \in I$. Si $k < n$, alors $n + m - k > m$, alors $y^{n+m-k} \in I$, d'où $x^k y^{n+m-k} \in I$. Par conséquent, $(x + y)^{n+m} \in I$, alors $x + y \in \sqrt{I}$. Si $x^n \in I$, alors $(-x)^n = (-1)^n x^n \in I$, alors \sqrt{I} est un sous-groupe additif de R . Si $x^n \in I$ et $y \in R$, alors $(yx)^n = y^n x^n \in I$, où on utilise la commutativité de R . Alors \sqrt{I} est un idéal.

- (b) Si $4 \mid x^n$, alors $2 \mid x^n$. Donc $2 \mid x$ ou $2 \mid x^{n-1}$. De toute façon, $2 \mid x$. Par contre, si $2 \mid x$, alors $4 \mid x^2$. Par conséquent, $\sqrt{4\mathbf{Z}} = 2\mathbf{Z}$.

Si $18 \mid x^n$, alors $2 \mid x$ et $3 \mid x$, par l'argument ci-dessus. Donc $x \in 6\mathbf{Z}$. Par contre, si $x \in 6\mathbf{Z}$ alors $36 \mid x^2$, donc $x \in \sqrt{18\mathbf{Z}}$. On conclut que $\sqrt{18\mathbf{Z}} = 6\mathbf{Z}$.

On remarque que $72 = 2^3 \cdot 3^2$. Par l'argument usuel, on montre que $72 \mid x^n \Rightarrow 2 \mid x$ et $3 \mid x$, alors $x \in 6\mathbf{Z}$. Par contre, si $x \in 6\mathbf{Z}$, alors $6^3 = 3 \cdot 72 \mid x^3$. Alors $x^3 \in 72\mathbf{Z}$. Par conséquent, $\sqrt{72\mathbf{Z}} = 6\mathbf{Z}$.

Si $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ alors $\sqrt{m\mathbf{Z}} = p_1 \cdots p_r \mathbf{Z}$. En effet, si $m \mid x^k$ alors $p_i \mid x$ pour tout i , alors $\sqrt{m\mathbf{Z}} \subset p_1 \cdots p_r \mathbf{Z}$. Par contre, si $x \in p_1 \cdots p_r \mathbf{Z}$ et $\alpha = \max(\alpha_1, \dots, \alpha_r)$, alors $m \mid x^\alpha$, donc $p_1 \cdots p_r \mathbf{Z} \subset \sqrt{m\mathbf{Z}}$.

- (c) Si $x^n \in I \cap J$, alors $x^n \in I$ et $x^n \in J$, c-à-d $x \in \sqrt{I} \cap \sqrt{J}$. Donc $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. Si $x^m \in I$ et $x^m \in J$, alors $x^{m+n} = x^m x^n \in IJ$. Donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{IJ}$. Si $x^m \in IJ$, alors $x^m \in I \cap J$ par l'exercice 1(a) de la série 8. Donc $\sqrt{IJ} \subset \sqrt{I \cap J}$. Alors

$$\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J} \subset \sqrt{IJ} \subset \sqrt{I \cap J}$$

d'où $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{IJ}$.

3. (a) On définit $\varphi : \mathbf{Z}[x] \rightarrow \mathbf{Z}[i]$ par $\varphi(x) = i$. Alors

$$\varphi(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 i + \cdots + a_n i^n.$$

L'homomorphisme φ est surjectif, puisque $\varphi(a + bx) = a + bi$ pour tout $a, b \in \mathbf{Z}$. Puisque $i^2 = -1$, il s'ensuit que $x^2 + 1 \in \ker \varphi$. Par contre, supposons que $f(x) \in \ker \varphi$. On écrit $f(x) = a_0 + a_1 x + \cdots + a_{2n+1} x^{2n+1}$ (si nécessaire, on pose $a_{2n+1} = 0$). Puisque $i^2 = -1$,

$$\varphi(f(x)) = (a_0 - a_2 + \cdots + (-1)^n a_{2n}) + (a_1 - a_3 + \cdots + (-1)^n a_{2n+1})i = 0.$$

Alors

$$a_0 - a_2 + \cdots + (-1)^n a_{2n} = 0$$

et

$$a_1 - a_3 + \cdots + (-1)^n a_{2n+1} = 0.$$

En particulier, $a_0 = a_2 - a_4 + \cdots - (-1)^n a_{2n}$. Alors

$$\begin{aligned} a_0 + a_2x^2 + \cdots + a_{2n}x^{2n} &= (a_2 - a_4 + \cdots - (-1)^n a_{2n}) + a_2x^2 + \cdots + a_{2n}x^{2n} \\ &= a_2(1 + x^2) - a_4(1 - x^4) + \cdots - (-1)^n a_{2n}(1 - (-1)^n x^{2n}). \end{aligned}$$

Or,

$$1 - (-1)^k x^{2k} = 1 - (-x^2)^k = (1 - (-x^2))(1 + (-x^2) + \cdots + (-x^2)^{k-1})$$

alors $1 + x^2$ divise $a_0 + a_2x^2 + \cdots + a_{2n}x^{2n}$. Un argument pareille montre que $1 + x^2$ divise $a_1 + a_3x^3 + \cdots + a_{2n+1}x^{2n+1}$. Par conséquent, $1 + x^2 \mid f(x)$. Alors $\ker \varphi = (x^2 + 1)$ et φ définit un isomorphisme

$$\mathbf{Z}[x]/(x^2 + 1) \xrightarrow{\cong} \mathbf{Z}[i].$$

- (b) Supposons que $a + bi \in \mathbf{Z}[i]^*$. On peut résoudre directement l'équation $(a + bi)(c + di) = 1$; on trouve que $ac - bd = 1$ et $ad + bc = 0$. En utilisant le fait que $a, b, c, d \in \mathbf{Z}$, on trouve que soit $a = \pm 1$ et $b = 0$, soit $a = 0$ et $b = \pm 1$.

Alternativement, on peut profiter de l'application $N : \mathbf{Z}[i] - \{0\} \rightarrow \mathbf{Z}_+$, $N(a + bi) = a^2 + b^2$. On constate que $N(xy) = N(x)N(y)$ pour $x, y \in \mathbf{Z}[i]$, tous les deux non-nuls. En effet, c'est un calcul direct. Également, $N(1) = 1$. Si x est inversible, alors il existe y tel que $xy = 1$. Alors $1 = N(1) = N(xy) = N(x)N(y)$. Puisque $N(x), N(y) \in \mathbf{Z}_+$, il s'ensuit que $N(x) = N(y) = 1$. Si $x = a + bi$, alors $a^2 + b^2 = 1$. Donc $x \in \{\pm 1, \pm i\}$.

Alors, $\mathbf{Z}[i]^* = \{1, -1, i, -i\} \cong C_4$, engendré par i , puisque $i^2 = -1$, $i^3 = -i$, et $i^4 = 1$.

- (c) On constate que $Q(\mathbf{Z}[i]) \cong \mathbf{Q}[i] = \{x + yi \mid x, y \in \mathbf{Q}\}$. En effet, pour $a + bi, c + di \in \mathbf{Z}[i]$ avec $c + di \neq 0$,

$$\begin{aligned} \frac{a + bi}{c + di} &= (a + bi) \left(\frac{c - di}{c^2 + d^2} \right) \\ &= \left(\frac{ac + bd}{c^2 + d^2} \right) + \left(\frac{bc - ad}{c^2 + d^2} \right) i \\ &\in \mathbf{Q}[i] \end{aligned}$$

alors $Q(\mathbf{Z}[i]) \subset \mathbf{Q}[i]$. Par contre, si $(a/b) + (c/d)i \in \mathbf{Q}[i]$, alors

$$\frac{a}{b} + \frac{c}{d}i = \frac{ad + bci}{bd + 0i} \in Q(\mathbf{Z}[i]).$$

4. (a) Si $(r, s) \in R \times S$, alors $(r, s) \sim (r, s)$ puisque $rs - rs = 0$. Donc la relation est réflexive. Si $(r, s) \sim (r', s')$, disons $s''(rs' - sr') = 0$, alors $(-s'')(r's - s'r) = 0$ alors $(r', s') \sim (r, s)$ et la relation est symétrique. Supposons que $(r, s) \sim (r', s')$ et $(r', s') \sim (r'', s'')$. Alors il existe $t, t' \in R$ tels que $t(rs' - sr') = 0$ et $t'(r's'' - s'r'') = 0$. On peut supposer que $t = t'$ (sinon, on prend tt'). Alors $ts''(rs' - sr') = 0$ et $ts(r's'' - s'r'') = 0$. Donc $ts'(rs'' - sr'') = 0$ et la relation est transitive.
- (b) D'abord on montre que l'addition est bien définie, c-à-d qu'elle est indépendante du choix des représentants. Supposons que $(r_1, s_1) \sim (r'_1, s'_1)$ et $(r_2, s_2) \sim (r'_2, s'_2)$. Disons que $t_1(r_1s'_1 - s_1r'_1) = 0$ et $t_2(r_2s'_2 - s_2r'_2) = 0$. Alors

$$\begin{aligned} t_1t_2[(r_1s_2 + r_2s_1)s'_1s'_2 - s_1s_2(r'_1s'_2 + r'_2s'_1)] &= [t_1(r_1s'_1 - s_1r'_1)]t_2s_2s'_2 \\ &\quad + [t_2(r_2s'_2 - s_2r'_2)]t_1s_1s'_1 \\ &= 0. \end{aligned}$$

Donc $(r_1s_2 + r_2s_1, s_1s_2) \sim (r'_1s'_2 + r'_2s'_1, s'_1s'_2)$ et l'addition est bien définie. La multiplication est la même idée.

Maintenant on montre que $S^{-1}R$ est un groupe additif. L'élément neutre est $0/s$ (n'importe quel $s \in S$), puisque $(r_1 \cdot s + 0 \cdot s_1, s \cdot s_1) = (r_1s, ss_1) \sim (r_1, s_1)$, alors $r_1/s_1 + 0/s = r_1/s_1$. L'inverse additive de r/s est $(-r)/s$. L'addition est associative parce que l'addition dans R est associative et distributive par rapport à la multiplication.

L'associativité de la multiplication dans R implique celle de la multiplication dans $S^{-1}R$. Pareille pour la distributivité.

Enfin, $1 = s/s$ pour n'importe quel $s \in S$.

- (c) L'homomorphisme ι commute avec l'addition parce que la multiplication est distributive. Pour la multiplication,

$$\begin{aligned} \iota(rr') &= \frac{(rr')s}{s} \\ &= \frac{(rr')s}{s} \cdot 1 \\ &= \left(\frac{(rr')s}{s} \right) \left(\frac{s}{s} \right) \\ &= \frac{(rs)(r's)}{ss} \\ &= \left(\frac{rs}{s} \right) \left(\frac{r's}{s} \right) \\ &= \iota(r)\iota(r'). \end{aligned}$$

Alors ι est un homomorphisme d'anneaux. On peut montrer que $r \in \ker \iota$ si et seulement s'il existe $t \in S$ tel que $rt = 0$. Alors ι est injectif si et seulement si S ne contient aucun diviseur de zéro.

- (d) On pose $S = R - P$. Supposons que $x, y \in R$ vérifient $xy \notin S$, c-à-d $xy \in P$. Alors $x \in P$ où $y \in P$ puisque P est premier. Alors $x \notin S$ ou $y \notin S$. Ce qui est la contrapositive de « $x, y \in S \Rightarrow xy \in S$ ». Donc S est multiplicativement stable. En ce cas, l'anneau $S^{-1}R$ est souvent noté R_P .
- (e) Si R est intègre, alors $(r, s) \sim (r', s') \Leftrightarrow rs' - sr' = 0$, c-à-d on n'a plus besoin de s'' . La reste suit des définitions.
- (f) $S^{-1}\mathbf{Z}$ consiste en toute fraction réduite telle que p ne divise pas le dénominateur. Soit $M = p(S^{-1}\mathbf{Z})$. Alors $S^{-1}\mathbf{Z} - M$ consiste en toute fraction réduite telle que p ne divise ni le numérateur, ne le dénominateur. Si $a/b \in S^{-1}\mathbf{Z} - M$, alors $a \in S$, donc $b/a \in S^{-1}\mathbf{Z}$. Alors a/b est inversible. Par l'exercice 1, M est l'unique idéal maximal, d'où $R^{-1}\mathbf{Z}$ est local.
5. Tout d'abord, on remarque que $\varphi(R) \subset Z(T)$, car R est commutatif. Puisque $\varphi(S) \subset T^*$, on essaie de définir $\hat{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$. Il faut montrer que cette définition est indépendante du choix de représentant (r, s) de la classe r/s . Si $(r, s) \sim (r', s')$, alors il existe $s'' \in S$ tel que $s''(rs' - sr') = 0$. Alors

$$\begin{aligned} 0 &= \varphi(s'')(\varphi(r)\varphi(s') - \varphi(s)\varphi(r')) \\ \varphi(s'')\varphi(r)\varphi(s') &= \varphi(s'')\varphi(s)\varphi(r') \\ \varphi(r)\varphi(s)^{-1} &= \varphi(r')\varphi(s')^{-1} \end{aligned}$$

puisque $\varphi(s), \varphi(s'), \varphi(s'') \in T^*$. Alors $\hat{\varphi}$ est bien défini en tant qu'application $S^{-1}R \rightarrow T$. Il est un homomorphisme parce que φ en est un. Enfin, si $r \in R$, alors $\hat{\varphi}(\iota(r)) = \hat{\varphi}(rs/s) = \varphi(rs)\varphi(s)^{-1} = \varphi(r)\varphi(s)\varphi(s)^{-1} = \varphi(r)$.