CORRIGÉ DU PARTIEL D'ALGÈBRE I (USTC 2019-2020)

Exercice 1.
Soit $(E, \leq)$ un ensemble ordonné.

(1) Interpretez la phrase suivante en utilisant la langue logique mathématique (on n'utilise que "$\forall$, $\exists$, $\leq$, $=$, $\in$, et, ou, non", et aussi des variables et des parenthèses si nécessaire, mais on ne utilise pas "$\Rightarrow$") :
- Si E n'a pas d'élément maximal, alors E n'a pas d'élément minimun.

(2) Soit A un ensemble contenant au moins deux éléments. Soit $E = \mathcal{P}(A) \setminus \{\emptyset, A\}$ muni de l'ordre partiel "$\subseteq$", l'assertion précédent est-elle vraie? Pourquoi?

Solution.

(1) On traduit la phrase concernée comme

$$non(\exists x \in E\ \forall y \in E\ (x \leq y) \Rightarrow (y = x)) \Rightarrow non(\exists x \in E\ \forall y \in E\ x \leq y).$$

Comme "$P \Rightarrow Q$" s'écrit "$(non\ P)\ ou\ Q$", on trouve :

$$(\exists x \in E\ \forall y \in E\ (x \leq y) \Rightarrow (y = x))\ ou\ non(\exists x \in E\ \forall y \in E\ x \leq y),$$

ou encore :

$$(\exists x \in E\ \forall y \in E\ (non(x \leq y)\ ou\ (y = x)))\ ou\ (\forall x \in E\ \exists y \in E\ non(x \leq y)).$$

Attention! $non(x \leq y)$ n'est pas équivalent à ($y \leq x$ et $x \neq y$) puisque "$\leq$" n'est pas forcément un ordre total.

(2) C'est vraie. On fixe un élément $a \in A$, la partie $A \setminus \{a\} \in E$ est un élément maximal de E, l'assertion concernée est donc vraie.

Exercice 2.
Soit $\sim$ une relation d'équivalence sur l'ensemble E. On désigne la classe d'équivalence d'un élément $x \in E$ par $\bar{x}$. On définit une application de l'ensemble des parties de E vers lui-même $s : \mathcal{P}(E) \to \mathcal{P}(E)$ par $s(A) = \bigcup\limits_{x \in A} \bar{x}$

(1) Comparez A, $s(A)$ et $s(s(A))$. Justifier votre conclusion.

(2) Montrer que pour tout $x \in E$ on a : $x \in s(A) \iff \bar{x} \cap A \neq \emptyset$

(3) Montrer que $s(\bigcap\limits_{i \in I} A_i) \subseteq \bigcap\limits_{i \in I} s(A_i)$. De plus, en donnant une relation d'équivalence sur $E = \{1, 2\}$, expliquez que la contenance stricte peut avoir lieu.

Solution.
Rappelons que deux classes d'équivalence soit être disjointes soit être identiques.

(1) On a $A \subseteq s(A) = s(s(A))$. En fait, on trouve $A \subseteq s(A) \subseteq s(s(A))$ par définition. De plus, pour tout $y \in s(s(A)) = \bigcup_{x \in s(A)} \bar{x}$ il existe $x \in s(A)$ tel que $y \in \bar{x}$, alors $\bar{x} = \bar{y}$. Le fait que $x \in s(A)$ signifie que $x \in \bar{z}$ pour un certain $z \in A$. Donc $y \in \bar{x} = \bar{z} \subseteq s(A)$, ainsi que $s(s(A)) \subseteq s(A)$.

(2) Si $x \in s(A)$, il existe $y \in A$ tel que $x \in \bar{y}$, alors $\bar{x} = \bar{y}$ ainsi que $y \in \bar{x} \cap A$. Réciproquement, on prend $y \in \bar{x} \cap A$, alors $x \in \bar{x} = \bar{y} \subseteq s(A)$.

(3) Pour tout $x \in s(\bigcap_{i \in I} A_i)$ il existe $y \in \bigcap_{i \in I} A_i \subseteq A_i$ tel que $x \in \bar{y}$. Donc $x \in \bar{y} \subseteq s(A_i)$ pour tout $i \in I$, autrement dit $x \in \bigcap_{i \in I} s(A_i)$.
On définit $\sim$ comme la relation triviale sur E, autrement dit on a une seule classe d'équivalence. On pose $A_1 = \{1\}$ et $A_2 = \{2\}$. Alors $s(A_1 \cap A_2) = \emptyset$ mais $s(A_1) \cap s(A_2) = E$.

Exercice 3.
Dans cet exercice, on désigne A un anneau commutatif avec l'élément neutre 1 pour sa multiplication.

(1) Soit $I \subset A$ un idéal, énoncer la définition pour que "I est un idéal maximal d'anneau A".
(2) Si $a \in A$ est un élément inversible, qu'est-ce que c'est l'idéal (a) engendré par a? Existe-il un idéal maximal de A contenant a? Justifier vos assertions.
(3) Énoncer le lemme de Zorn.
(4) Si $a \in A$ n'est pas inversible, en utilisant le lemme de Zorn, montrer qu'il existe un idéal maximal de A contenant a.
(5) En résumant les résultats précédents, donner une caractérisation simple de la réunion des idéaux maximaux de A.

Solution.

(1) I est un élément maximal dans l'ensemble des idéaux propres de A. Autrement dit, l'idéal $I \neq A$ et si $J \neq A$ est un idéal contenant I alors $I = J$.
(2) Si $a \in A$ est inversible, alors pour tout $x \in A$ on a $x = xa^{-1}a \in (a)$, ainsi que $(a) = A$. Si un idéal maximal contient a, il contient $(a) = A$ qui est absurd. Donc il n'y a pas d'idéal maximal contenant a.
(3) Lemme de Zorn :
   - Soit $(\Omega, \leq)$ un ensemble ordonné non-vide. Si toute partie totalement ordonnée de Ω admet un majorant dans Ω, alors Ω admet un élément maximal.
(4) Supposont que $a \in A$ n'est pas inversible. On considère $\Omega = \{I \subsetneq A \text{ idéaux contenant } a\}$. L'ensemble Ω est non-vide car $(a) \in \Omega$. Pour toute partie $\{I_\lambda\}_{\lambda \in \Lambda}$ totalement ordonnée par $\subseteq$ de Ω. L'idéal $J = \bigcup_{\lambda \in \Lambda} I_\lambda$ est bien un idéal propre de A et il contient a, c'est un majorant de $\{I_\lambda\}_{\lambda \in \Lambda}$ dans Ω. D'après le lemme de Zorn, l'ensemble Ω admet un élément maximal qui est a fortiori un idéal maximal de A.
(5) D'après (2) et (4), on trouve $\displaystyle\bigcup_{\mathfrak{m} \subseteq A \text{ id. max.}} \mathfrak{m} = A \setminus A^\times$. **Remarque.** Géométriquement, cela signifie que, sur une surface de Riemann S, si on pose A comme l'ensemble des fonctions holomorphes sur S, $1/f$ est holomorphe si et seulement si la fonction holomorphe f ne s'annule pas sur S. Ou bien encore plus simple $1/f$ a un sens pour une fonction f si et seulement si f n'admet pas de racine.

Exercice 4.

(1) Soit K un corps, en utilisant la méthode du pivot de Gauss, déterminer une condition nécessaire et suffisante sur les coefficients $(\alpha, \beta, \gamma) \in K^3$ telles que pour toute triple

$(a, b, c) \in K^3$ le système linéaire suivant admet une seule solution.

$$\begin{cases} x + \alpha y + \alpha^2 z &= a \\ x + \beta y + \beta^2 z &= b \\ x + \gamma y + \gamma^2 z &= c \end{cases}$$

(2) Énoncer une conjecture pour généraliser la première question au cas où le système admet n inconnues et n équations. (On ne demande pas de démonstration.)
(3) Soit $P \in \mathbb{C}[X]$ un polynôme, si $\alpha \in \mathbb{C}$ est une racine multiple de P, montrer que $(X - \alpha)$ divise le pgcd de P et P'.
(4) Soient P et Q des polynômes de $\mathbb{Q}[X]$, si P et Q sont premiers entre eux dans $\mathbb{Q}[X]$, montrer que P et Q sont aussi premiers entre eux dans $\mathbb{C}[X]$.
(5) En appliquant les deux résultats précédents, montrer que si le polynôme $P \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$, alors il n'a pas de racine multiple dans $\mathbb{C}$.
(6) Étant donnés A et B des polynômes unitaires irréductibles non-constants dans $\mathbb{Q}[X]$. Énoncer le résultat suivant en utilisant la langue structurielle d'algèbre
   - Pour tous polynômes $U \in \mathbb{Q}[X]$ et $V \in \mathbb{Q}[X]$ tels que $\deg(U) < \deg(A)$ et $\deg(V) < \deg(B)$, il existe un polynôme $P \in \mathbb{Q}[X]$ tel que le reste de la division euclidienne de P par A (respectivement B) vaut U (respectivement V). De plus, le reste R de la division euclidienne de P par AB est uniquement déterminé par U et V.

   Auquel résultat sur $\mathbb{Z}$ est-ce que cet énoncé est analoque?
(7) On admet l'existence du résultat précédent, en considérant le système linéaire des équation pour les coefficients de R, démontrer la unicité du résultat précédent. On pourra admettre des conclusions et la conjecture des questions précédentes.

Solution.

(1) On considère la matrice associée

$$\left(\begin{array}{ccc|c} 1 & \alpha & \alpha^2 & a \\ 1 & \beta & \beta^2 & b \\ 1 & \gamma & \gamma^2 & c \end{array}\right)$$

On effectue la méthode du pivot de Gauss, après $L_2 \leftarrow L_2 - L_1$ et $L_3 \leftarrow L_3 - L_1$ on trouve

$$\left(\begin{array}{ccc|c} 1 & \alpha & \alpha^2 & a \\ 0 & \beta-\alpha & (\beta-\alpha)(\beta+\alpha) & b-a \\ 0 & \gamma-\alpha & (\gamma-\alpha)(\gamma+\alpha) & c-a \end{array}\right)$$

La condition que ce système admet toujours une solution implique que $\alpha \neq \beta$. Comme la question est symétrique par rapport à α, β, γ, on trouve donc une condition nécessaire "α, β, γ deux à deux distincts". Sous cette condition, on peut continuer simplifier la matrice, on trouve

$$\cdots \sim \left(\begin{array}{ccc|c} 1 & \alpha & \alpha^2 & a \\ 0 & 1 & \beta+\alpha & \frac{b-a}{\beta-\alpha} \\ 0 & 1 & \gamma+\alpha & \frac{c-a}{\gamma-\alpha} \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & \alpha & \alpha^2 & a \\ 0 & 1 & \beta+\alpha & \frac{b-a}{\beta-\alpha} \\ 0 & 0 & \gamma-\beta & \frac{c-a}{\gamma-\alpha} - \frac{b-a}{\beta-\alpha} \end{array}\right)$$

Le système linéaire associé à cette dernière matrice est toujours compatible et sa solution est unique.

(2) **Conjecture.** Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des éléments de K deux à deux distincts. Alors le système linéaire suivant admet toujours une unique solution.

$$\begin{cases} x_1 + \alpha_1 x_2 + \cdots + \alpha_1^{n-1} x_n & = & a_1 \\ x_1 + \alpha_2 x_2 + \cdots + \alpha_2^{n-1} x_n & = & a_2 \\ \vdots & = & \vdots \\ x_1 + \alpha_n x_2 + \cdots + \alpha_n^{n-1} x_n & = & a_n \end{cases}$$

(3) Il existe $Q \in \mathbb{C}[X]$ tel que $P = (X-\alpha)^2 Q$. Alors $P' = 2(X-\alpha)Q + (X-\alpha)^2 Q'$ est un multiple de $(X-\alpha)$.

(4) Si P et Q sont premiers entre eux dans $\mathbb{Q}[X]$, il existe $(S,T) \in \mathbb{Q}[X]^2$ tels que $PS + QT = 1$ d'après le théorème de Bézout. C'est également un identité dans $\mathbb{C}[X]$. Donc P et Q sont premiers entre eux dans $\mathbb{C}[X]$.

(5) Comme P est irréductible sur $\mathbb{Q}$ et $\deg(P) > \deg(P')$, les polynômes P et P' sont premiers entre eux dans $\mathbb{Q}[X]$. D'après 4 et 3, ils sont premiers entre eux dans $\mathbb{C}[X]$ et P n'admet alors pas de racine multiple dans $\mathbb{C}$.

(6)
- Soient A et B des polynômes irréductibles unitaires non-constants distincts. L'homomorphisme d'anneaux

$$\mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]/(A) \times \mathbb{Q}[X]/(B),\ P \mapsto (P \mod A,\ P \mod B)$$

est une surjection. De plus, il factorise à travers

$$\mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]/(AB),\ P \mapsto P \mod AB$$

et il induit un isomorphisme d'anneaux

$$\mathbb{Q}[X]/(AB) \longrightarrow \mathbb{Q}[X]/(A) \times \mathbb{Q}[X]/(B).$$

Il est analoque au théorème/lemme chinois.

(7) Soit $R = t_0 + t_1 X + t_2 X^2 + \cdots + t_{r+s-1} X^{r+s-1}$ le reste de la division euclidienne de P par AB, où $r = \deg(A)$ et $s = \deg(B)$. Il existe alors $(Q, Q_1, Q_2) \in \mathbb{Q}[X]^3$ tels que

$$P = AQ_1 + U,$$
$$P = BQ_2 + V,$$
$$P = ABQ + R.$$

Soient $\alpha_1, \ldots, \alpha_r$ les racines complexes de A et soient $\alpha_{r+1}, \ldots, \alpha_{r+s}$ les racines complexes de B. Comme A et B sont irréductibles sur $\mathbb{Q}$, ils n'ont pas de racine multiple d'après 5. Comme A et B sont premiers entre eux sur $\mathbb{Q}$, ils n'ont pas de racine commune dans $\mathbb{C}$ d'après 4. Alors les α_i sont deux à deux distincts. En les substituant dans les trois équations ci-dessus, on trouve un système linéaire à inconnues $t_0, t_1, \ldots, t_{r+s-1}$ de $r+s$ équations du type dans la question 2, d'où l'unicité de la solution.