Anneaux et arithmétique (ANAR)
CC 1 - Groupe magistère (1h15)

Aucun document ni appareil électronique autorisé

21 février 2022

Exercice 1. (4pts) Soit A un anneau commutatif unitaire intègre.

1) a) (2pts) Montrer que $(A[X])^\times = A^\times$. *Correction : Le sens $\supseteq$ est immédiat. Soit maintenant $P \in A[X]^\times$. Il existe donc $Q \in A[X]$ tel que $PQ = 1_A$. Puisque A est intègre, on a $\deg PQ = \deg P \deg Q = 0_A$ donc (encore puisque A est intègre) $\deg P$ ou $\deg Q = 0$. Puisque Q est arbitraire on en déduit que $\deg P = 0$ donc il existe $a \in A$ tel que $P = a$. De l'égalité $aQ = 1_A$ on en déduit $aQ(0) = 1_A$ donc puisque A est commutatif on obtient $a \in A^\times$.*

   b) (1pt) En déduire que si k est un corps alors $(k[X_1, \dots, X_n])^\times = k^\times$. *Correction : De proche en proche, puisque $k[X_1, \dots, X_n]$ est commutatif unitaire intègre (car k l'est) on en déduit que $k[X_1, \dots, X_n]^\times = k[X_1, \dots, X_{n-1}]^\times = k[X_1]^\times = k^\times$.*

2) (1pt) Soit $P \in A[X]$ irréductible et soit $a \in A$. Montrer que $P(X + a) \in A[X]$ est irréductible. *Correction : Soient $Q, R \in A[X]$ tels que $P(X + a) = QR$. Alors $P(X) = Q(X - a)R(X - a)$ donc puisque P est irréductible on en déduit que $Q(X-a) \in A[X]^\times$ ou $R(X-a) \in A[X]^\times$, donc par 1)a) on en déduit que $Q(X-a)$ ou $R(X - a)$ est un inversible de A, donc $Q(X)$ ou $R(X)$ également et l'un des deux est donc un inversible de $A[X]^\times$.*

Exercice 2. (12pts) Soit A un anneau commutatif unitaire. Le *radical de Jacobson* de A, noté $J(A)$, est l'intersection des idéaux maximaux de A.

1) (1pt) Déterminer $J(\mathbb{Q})$. *Correction : Si I est un idéal de $\mathbb{Q}$, s'il existe $x \neq 0$ dans I alors $xx^{-1} = 1 \in I$ donc $I = \mathbb{Q}$. Ainsi, les seuls idéaux de $\mathbb{Q}$ sont (0) et $\mathbb{Q}$ donc (0) est l'unique idéal maximal donc $J(\mathbb{Q}) = (0)$.*

2) On veut montrer que $J(\mathbb{Z}) = \{0\}$.

   a) (.5pt) Rappeler (sans démonstration) la forme des idéaux de $\mathbb{Z}$. *Correction : Ce sont les $n\mathbb{Z}$ pour $n \geq 0$.*

   b) (2pts) Déterminer les idéaux premiers de $\mathbb{Z}$. *Correction : Montrons que ce sont les $p\mathbb{Z}$ pour p premier ou $p = 0$. L'idéal (0) est bien premier puisque $\mathbb{Z}$ est intègre, et si maintenant p est premier alors si $ab \in p\mathbb{Z}$ alors $p \mid ab$ donc $p \mid a$ ou $p \mid b$ puisque p est premier donc $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$, donc $p\mathbb{Z}$ est un idéal premier. Réciproquement, supposons que $n\mathbb{Z}$ est un idéal premier. Si $n = 0$ il n'y a rien à faire, le cas $n = 1$ est impossible puisque $\mathbb{Z}$ n'est pas premier par définition, donc on suppose $n \geq 2$. Si n n'est pas premier, on peut écrire $n = ab$ pour $a, b \geq 2$. On a alors $ab = n \in n\mathbb{Z}$ mais $a, b \notin n\mathbb{Z}$ ce qui est absurde.*

   c) (1pt) En déduire les idéaux maximaux. *Correction : Tout idéal maximal est premier, donc on cherche parmi les $p\mathbb{Z}$ pour $p = 0$ ou p premier. Bien sûr (0) n'est pas maximal car $(0) \subsetneq 2\mathbb{Z}$, et sinon $p\mathbb{Z}$ est maximal puisque si $p\mathbb{Z} \subseteq n\mathbb{Z}$ alors $n \mid p$ donc $n = 1$ (auquel cas $n\mathbb{Z} = \mathbb{Z}$) ou $n = p$.*

d) (1pt) Conclure. *Correction : On a donc* $J(\mathbb{Z}) = \cap_p p\mathbb{Z}$ *où* p *parcourt l'ensemble des nombres premiers. Si* n *est dans cette intersection alors* $p \mid n$ *pour tout entier premier* p*. Or, si* $n \neq 0$ *alors* n *ne possède qu'un nombre fini de facteurs premiers, ce qui implique que* $J(\mathbb{Z}) \subseteq (0)$*. L'implication réciproque est immédiate donc* $J(\mathbb{Z}) = (0)$*.*

3) Soit $a \in A$.

a) (.5pt) Montrer que si a est contenu dans un idéal maximal de A alors $a \notin A^\times$. *Correction : On suppose* $a \in \mathfrak{m}$*. Si* $a \in A^\times$ *alors* $1_A = a^{-1}a \in \mathfrak{m}$ *donc* $\mathfrak{m} = A$ *ce qui est impossible.*

b) (1pt) Montrer la réciproque. *Correction : Si* $a \notin A^\times$ *alors* $(a) \subsetneq A$ *puisque* $1_A \notin (a)$*. Ainsi l'idéal* (a) *est strict donc est inclus dans un idéal maximal par le théorème de Krull (l'anneau* A *étant unitaire).*

4) (2pts) Si $a \notin J(A)$, montrer qu'il existe $b \in A$ tel que $1_A - ab \notin A^\times$. *Correction : Par définition, il existe un idéal maximal tel que* $a \notin \mathfrak{m}$*. Ainsi, on a* $\mathfrak{m} + (a) = A$ *donc il existe* $b \in A$ *tel que* $1_A - ab \in \mathfrak{m}$*. On conclut par la question 3)a) puisque* $\mathfrak{m}$ *est maximal.*

5) (2pts) Montrer la réciproque et en déduire une description de $J(A)$. *Correction : Soit* $b \in A$ *tel que* $1_A - ab \notin A^\times$*. Par la question 3)b), on sait qu'il existe un idéal maximal* $\mathfrak{m}$ *tel que* $1_A - ab \in \mathfrak{m}$*. On a ainsi* $a \notin \mathfrak{m}$ *puisque sinon on aurait* $1_A \in \mathfrak{m}$*. On en déduit que* $a \notin J(A)$*. On conclut que* $J(A) = \{a \in A : 1 - ab \in A^\times$ *pour tout* $b \in A\}$*.*

6) (1pt) En déduire le radical de Jacobson de $\mathbb{Z}/2\mathbb{Z}[X]$. *Correction : D'après l'Exercice 1, puisque* $\mathbb{Z}/2\mathbb{Z}$ *est commutatif unitaire intègre on a* $\mathbb{Z}/2\mathbb{Z}[X]^\times = (\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$*. Ainsi, un polynôme* P *est dans le radical de Jacobson si et seulement si pour tout polynôme* Q *on a* $1 - PQ = 1$ *donc si et seulement si* $PQ = 0$ *pour tout polynôme* Q *donc* $P = 0$ *(il suffit de prendre* $Q = 1$*).*

Exercice 3 (Critère d'Eisenstein)**.** (10pts) Soit p un nombre premier et soit $n \geq 1$.

1) Soit k un corps.

a) (1pt) Soit $P \in k[X]$. Montrer que si $\alpha \in k$ est racine de P alors $X - \alpha$ divise P dans $k[X]$. *Correction : La division euclidienne de* P *par* $X - \alpha$ *dans* $k[X]$ *donne* $P = (X - \alpha)Q + R$ *avec* $\deg R < \deg(X - \alpha) = 1$*, donc* R *est une constante. En évaluant l'égalité précédente en* α *on obtient* $0_k = 0_k Q(\alpha) + R$ *donc* $R = 0_k$*, ainsi on a bien* $X - \alpha \mid P$*.*

b) (1pt) En déduire que si $P, Q \in k[X]$ sont deux polynômes tels que $PQ = X^n$ alors il existe $a, b \geq 0$ avec $a+b = n$ et $\lambda \in k^\times$ tels que $P = \lambda X^a$ et $Q = \lambda^{-1}X^b$. *Correction : On montre le résultat par récurrence sur* $n \geq 0$*. Si* $n = 0$ *alors en passant au degré on trouve* $\deg P = \deg Q = 0$ *donc avec* $\lambda \in k$ *tel que* $P = \lambda$ *on trouve* $\lambda Q(0_k) = 1_k$ *donc* $\lambda \in k^\times$ *et* $Q = \lambda^{-1}$*. On suppose maintenant* $n \geq 1$*. On a* $P(0_k)Q(0_k) = 0_k$ *donc puisque* k *est intègre on a* $P(0_k) = 0_k$ *ou* $Q(0_k) = 0_k$*, ainsi* $X \mid P$ *ou* $X \mid Q$ *par la question précédente. Quitte à renommer on peut supposer* $X \mid P$*, et soit* $P_1 \in k[X]$ *tel que* $P = XP_1$*. On trouve alors* $P_1 Q = X^{n-1}$ *donc par hypothèse de récurrence on a* $P_1 = \lambda X^{a-1}$ *et* $Q = \lambda^{-1}X^b$ *pour* $(a-1)+b = n-1$*, donc on a bien* $P = \lambda X^a$ *et* $Q = \lambda^{-1}X^b$ *avec* $a + b = n$*.*

2) Soit $P = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{Z}[X]$. On suppose que $p \mid a_k$ pour $k \in \{0, \ldots, n-1\}$.

a) Soient $Q, R \in \mathbb{Z}[X]$ non constants tels que $P = QR$.

i) (2pts) En passant dans $\mathbb{Z}/p\mathbb{Z}[X]$, montrer que tous les coefficients de Q et R, excepté les coefficients dominants, sont divisibles par p. *Correction : On a* $\overline{P} = \overline{QR}$*. Par hypothèse on a* $\overline{P} = X^n \in \mathbb{Z}/p\mathbb{Z}[X]$ *donc par la*

question précédente on en déduit qu'il existe $\lambda \in (\mathbb{Z}/p\mathbb{Z})^\times$ *et* $a, b \geq 0$ *avec* $a+b=n$ *tels que* $\overline{Q} = \lambda X^a$ *et* $\overline{R} = \lambda^{-1} X^b$. *En remarquant que le produit des coefficient dominants de* Q *et* R *fait* 1 *(le coefficient dominant de* P*), ces coefficients dominants sont nécessairement* ± 1 *donc en particulier non nuls dans* $\mathbb{Z}/p\mathbb{Z}$, *et ainsi* $a = \deg Q \geq 1$ *et* $b = \deg R \geq 1$. *On obtient donc le résultat escompté.*

ii) (1pt) En déduire que $p^2 \mid a_0$. *Correction : On a* $a_0 = P(0) = Q(0)R(0)$ *et par la question précédente on a* $p \mid Q(0)$ *et* $p \mid R(0)$ *(les polynômes* Q *et* R *ne sont pas constants par hypothèse donc de degré* ≥ 1*).*

b) (2pts) En déduire que si $p^2 \nmid a_0$ alors P est irréductible dans $\mathbb{Z}[X]$. *Correction : On a* $\deg P = n \geq 1$ *donc* P *est non nul et non inversible (par l'Exercice 1). Soient* $Q, R \in \mathbb{Z}[X]$ *tels que* $P = QR$. *Par hypothèse et par la question a), nécessairement* Q *ou* R *est constant. Par symétrie, on peut supposer* $Q = n \in \mathbb{Z}$. *On a donc* $P = nR$, *mais* P *étant unitaire (et* $\mathbb{Z}$ *intègre) on en déduit que* $n \deg(R) = 1$ *donc* $n \in \mathbb{Z}^\times$ *donc* $n = \pm 1$. *Ainsi* $Q = \pm 1 \in \mathbb{Z}[X]^\times$ *et finalement* P *est irréductible dans* $\mathbb{Z}[X]$.

3) (1pt) Exhiber un polynôme irréductible de $\mathbb{Z}[X]$ de degré n. *Correction : Le polynôme* $X^n + p$ *vérifie le critère d'Eisenstein.*

4) (2pts) Montrer que $\Phi_p \coloneqq X^{p-1} + X^{p-2} + \cdots + X + 1$ est irréductible dans $\mathbb{Z}[X]$. *Correction : On peut appliquer le critère d'Eisenstein à* $\Phi_p(X+1)$, *puisque :*

$$\begin{aligned}
\Phi_p(X+1) &= \sum_{k=0}^{p-1} (X+1)^k \\
&= \sum_{k=0}^{p-1} \sum_{\ell=0}^{k} \binom{k}{\ell} X^\ell \\
&= \sum_{\ell=0}^{p-1} \left(\sum_{k=\ell}^{p-1} \binom{k}{\ell} \right) X^\ell.
\end{aligned}$$

En rappelant la formule du triangle de Pascal $\binom{n-1}{a-1} + \binom{n-1}{a} = \binom{n}{a}$, *on trouve que*

$$\begin{aligned}
\sum_{k=\ell}^{p-1} \binom{k}{\ell} &= \binom{\ell}{\ell} + \sum_{k=\ell+1}^{p-1} \binom{k}{\ell} \\
&= \binom{\ell+1}{\ell+1} + \sum_{k=\ell+1}^{p-1} \binom{k}{\ell} \\
&= \binom{\ell+2}{\ell+1} + \sum_{k=\ell+2}^{p-1} \binom{k}{\ell} \\
&= \binom{\ell+3}{\ell+1} + \sum_{k=\ell+3}^{p-1} \binom{k}{\ell} \\
&= \dots \\
&= \binom{p-1}{\ell+1} + \sum_{k=p-1}^{p-1} \binom{k}{\ell} \\
&= \binom{p}{\ell+1}.
\end{aligned}$$

Remarquons que l'on pouvait aussi passer par $\mathbb{Q}(X)$, *en remarquant que* $\Phi_p(X) =$

$\frac{X^p-1}{X-1}$:

$$\begin{aligned}\Phi_p(X+1) &= \frac{(X+1)^p-1}{X+1-1} \\ &= X^{-1}\left((X+1)^p-1\right) \\ &= X^{-1}\sum_{\ell=1}^{p}\binom{p}{\ell}X^\ell \\ &= \sum_{\ell=0}^{p-1}\binom{p}{\ell+1}X^\ell.\end{aligned}$$

Ainsi, on a $\Phi_p(X+1) = \sum_{\ell=0}^{p-1}\binom{p}{\ell+1}X^\ell$. *Le coefficient dominant est* $\binom{p}{p} = 1$, *le coefficient constant est* $\binom{p}{1} = p$, *les autres coefficients sont* $\binom{p}{\ell+1}$ *pour* $1 \leq \ell < p-1$ *donc sont bien divisibles par* p. *On en déduit que* $\Phi_p(X+1)$ *vérifie le critère d'Eisenstein, donc est irréductible dans* $\mathbb{Z}[X]$, *donc* $\Phi_p(X)$ *également par l'Exercice 1.*