École Polytechnique 2009-2010

Théorie de Galois

Corrigé de la Feuille d'exercices 2

Exercice 1.

(i) Soit π la projection naturelle de A sur A/I Les assertions suivantes sont clairement équivalentes :

I premier,

$\forall x, y \in A$, $\pi(x)\pi(y) = 0$ implique $\pi(x) = 0$ ou $\pi(y) = 0$,

$\forall X, Y \in A/I$, $XY = 0$ implique $X = 0$ ou $Y = 0$,

A/I est intègre.

(ii) Si I est maximal, soit $X \in (A/I) \setminus \{0\}$. Soit $x \in A$ un représentant de X. Alors l'idéal $I + Ax$ contient I strictement, et donc $I + Ax = A$. Donc $1 = i + ax$ avec $i \in I$ et $a \in A$. Donc $1 = \pi(a)X$ et X a un inverse dans A/I.

Maintenant si A/I est un corps, soit J un idéal de A contenant I strictement. Soit $x \in J \setminus I$. Alors $\pi(x) \neq 0$ a un inverse Y dans A/I. Soit $y \in A$ un représentant de Y. Alors il existe $i \in I$ tel que $1 = i + yx$. Donc $1 \in J$ et $A = J$.

(iii) Si I est maximal, alors A/I est un corps donc intègre. Donc I est premier.

(iv) Si $\mathbf{Z}/n\mathbf{Z}$ est un corps, il est intègre. Montrons que

$\mathbf{Z}/n\mathbf{Z}$ intègre $\Rightarrow$ n premier $\Rightarrow$ $\mathbf{Z}/n\mathbf{Z}$ corps.

On aura alors l'équivalence des trois assersions. Si $\mathbf{Z}/n\mathbf{Z}$ est intègre, alors $n\mathbf{Z}$ est premier. Si $n = pq$ avec $1 < p, q < n$, alors $pq = 0$ dans $\mathbf{Z}/n\mathbf{Z}$, contradiction avec l'intégrité. Donc n est premier. Maintenant si n est premier, soit m tel que $n\mathbf{Z} \subsetneq m\mathbf{Z}$. Alors m divise n et $m < n$, donc $m = 1$. Donc $n\mathbf{Z}$ est maximal et $\mathbf{Z}/n\mathbf{Z}$ est un corps.

Exercice 2.

(i) Ce sont les polynômes $P(T) = \sum_{0 \leq i \leq n} a_i T^i$ avec a_0 inversible et pour $i \geq 1$, a_i nilpotent. En effet pour un tel polynôme, $a_0^{-1}(\sum_{N \geq 0}(\sum_{1 \leq i \leq n} a_0^{-1} a_i T^i)^N)$ est un inverse dans $\mathbf{Z}[T]$. Réciproquement, si $P(T)$ a un inverse $Q(T) = \sum_{0 \leq i \leq m} q_i T^i$, on a d'abord $a_0 q_0 = 1$ donc a_0 est inversible. On identifie alors par récurrence les coefficients de $Q(T)$ avec la formule ci-dessus. Le fait Q n'a qu'un nombre fini de terme implique que les a_i sont nilpotents pour $i > 0$.

(ii) Comme $A \subset A[T]$, l'intégrité de A découle clairement de celle de $A[T]$. Maintenant si A est intègre, soient $P(T), Q(T) \in A[T]$ tels que $P(T)Q(T) = 0$. Si $P(T)$ et $Q(T)$ sont non nuls, le produit de leurs coefficients dominants est nul et donc l'un des deux est nul, contradiction.

(iii) Soient P, Q primitifs. Supposons qu'il existe $p > 1$ premier qui divise tous les coefficients de PQ. Alors dans $(\mathbf{Z}/p\mathbf{Z})[T]$, $P(T)Q(T) = 0$. Or $(\mathbf{Z}/p\mathbf{Z})[T]$ est intègre car $\mathbf{Z}/p\mathbf{Z}$ est intègre. Donc $P(T) = 0$ ou $Q(T) = 0$ dans $(\mathbf{Z}/p\mathbf{Z})[T]$, contradiction car ils sont primitifs.

(iv) En considérant le plus petit commun multiple des dénominateurs des coefficients de P, on peut écrire $P = R/r$ avec $r \in \mathbf{Z}$ et $R \in \mathbf{Z}[T]$. Alors en considérant le plus grand commun diviseur des coefficients de R, on obtient $P = Qr'$ avec $r' \in \mathbf{Q}$ et $Q \in \mathbf{Z}[T]$ primitif. Si $r' < 0$, il suffit d'écrire $P = (-Q)(-r')$. Pour l'unité, on suppose qu'on a deux écritures $P = Q_1 r_1 = Q_2 r_2$. Alors on identifie le plus grand commun diviseur des

coefficients, ce qui donne $r_1 = r_2$. Ceci implique $Q_1 = Q_2$. Si $P \in \mathbf{Z}[T]$, on considère le plus grand commun diviseur r des coefficients de P. Alors $P = r(P/r)$ avec P/r primitif, donc $r = c(P) \in \mathbf{Z}$.

(v) On écrit $PQ = c(P)c(Q)R_1R_2$ avec R_1, R_2 primitifs. Alors R_1R_2 est primitif, donc par unicité du contenu, $c(PQ) = c(P)c(Q)$.

Exercice 3.

(i) Si P est irréductible dans $\mathbf{Z}[T]$, alors il est primitif sinon on aurait une décomposition $P = c(P)Q$. Si il se factorisait dans $\mathbf{Q}[T]$ sous la forme $P = P_1P_2$ en polynômes de degré non nul, on aurait $P = c(P_1P_2)Q_1Q_2 = Q_1Q_2$, contradiction. Maintenant si P est primitif et irréductible dans $\mathbf{Q}[T]$, on écrit $P = P_1P_2$ dans $\mathbf{Z}[T]$. Alors $c(P_1)c(P_2) = 1$ donc $c(P_1) = c(P_2) = 1$ dans $\mathbf{Z}$, donc P_1 et P_2 sont inversibles dans $\mathbf{Z}[T]$ ou de degrés non nuls. Le deuxième cas n'est pas possible par irréductibilité dans $\mathbf{Q}[T]$.

(ii) Supposons que $P = QR$ dans $\mathbf{Z}[T]$. Alors dans $(\mathbf{Z}/p\mathbf{Z})[T]$ on a $QR = a_nT^n$. Donc les coefficients de Q et de R non dominants sont divisibles par p. Comme p^2 ne divise pas a_0, Q ou R est de degré 0. Or $1 = c(Q)c(R)$, donc $c(Q) = c(R) = 1$, et donc Q ou R est inversible dans $\mathbf{Z}[T]$.

(iii) La preuve est analogue.