Université Pierre et Marie Curie 2006–2007

LM220 Maths-Info groupes 1, 2 et 5

Devoir maison n° 2 : un corrigé

1 Lemme de Gauss

Remarque préliminaire. On constate que pour $a \in \mathbf{Z}$ et $P \in \mathbf{Z}[X]$, on a $c(aP) = a \cdot c(P)$. Ce fait, découlant de propriétés élémentaires du PGCD, sera abondamment utilisé dans les deux premières sections.

1.1 On a, par définition, $c_k = \sum_{i+j=k} a_i b_j$.

1.2 Le cas P et Q primitifs.

1.2.1 L'ensemble des entiers i tels que $p \nmid a_i$ est non vide : en effet, dans le cas contraire, p diviserait $c(P) = 1$, ce qui est absurde. Cet ensemble admet donc un plus petit élément, qui est le i_0 recherché. On procède de même pour j_0.

1.2.2 On a supposé que $p \mid c(PQ)$. Ainsi, p divise chacun des coefficients de PQ donc, en particulier, $c_{i_0+j_0}$. Par ailleurs, on a

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \overbrace{\sum_{\substack{i+j=i_0+j_0 \\ i<i_0}} a_i b_j}^{A} + \overbrace{\sum_{\substack{i+j=i_0+j_0 \\ j<j_0}} a_i b_j}^{B} .$$

En effet, si $i + j = i_0 + j_0$, on a soit $i = i_0$ et $j = j_0$, soit $i < i_0$ et $j > j_0$, soit $i > i_0$ et $j < j_0$. Par définition de i_0, on voit que $p \mid A$, et par celle de j_0, que $p \mid B$. Ainsi p divise $a_{i_0} b_{j_0} = c_{i_0+j_0} - A - B$. Mais ceci est absurde car p est premier et ne divise ni a_{i_0} ni b_{j_0}.

1.2.3 Par la question précédente, aucun nombre premier ne divise $c(PQ)$. Ce dernier est donc égal à 1.

1.3 On pose $\widetilde{P} = P/c(P)$. Comme $c(P)$ divise chacun des coefficients de P, on a bien $\widetilde{P} \in \mathbf{Z}[X]$. De plus, $c(P) = c\big(c(P) \cdot \widetilde{P}\big) = c(P) \cdot c(\widetilde{P})$ par la remarque préliminaire. En simplifiant, il vient $c(\widetilde{P}) = 1$, et $\widetilde{P}$ est primitif. On raisonne de même pour $\widetilde{Q}$.

1.4 Pour P et Q quelconques, on choisit $\widetilde{P}$ et $\widetilde{Q}$ comme à la question précédente. On a alors $PQ = c(P)c(Q)\widetilde{P}\widetilde{Q}$, et

$$c(PQ) = c(P)c(Q)c(\widetilde{P}\widetilde{Q}) = c(P)c(Q) \ ,$$

où la deuxième égalité découle de la question 1.2.

2 Irréductibilité dans $\mathbf{Z}[X]$ et $\mathbf{Q}[X]$

2.1 On écrit $Q = \sum_{i=0}^{d} p_i/q_i X^i$, avec pour tout i, $p_i \wedge q_i = 1$. On pose alors $m = \mathrm{PPCM}(q_0, \dots, q_d)$.

2.1.1 Par définition, $q_i \mid m$ pour tout i, donc m/q_i est entier et $m(p_i/q_i)$ aussi. Ainsi, les coefficients de mQ sont entiers.

2.1.2 On a $c(mQ) = c(\widetilde{Q} \cdot c(mQ)) = c(\widetilde{Q}) \cdot c(mQ)$. Ainsi, $\widetilde{Q}$ est primitif.

2.1.3 On raisonne par l'absurde en supposant qu'il existe un nombre premier p qui divise à la fois m et $c(mQ)$. Comme m est le PPCM des q_i, il existe un entier i_0 tel que $v_p(m) = v_p(q_{i_0})$. Ainsi, $v_p(m/q_{i_0}) = 0$, c'est-à-dire $p \nmid (m/q_{i_0})$. Par ailleurs, p divise chaque coefficient de mQ puisqu'il divise leur PGCD. En particulier p divise $(m/q_{i_0})p_{i_0}$. Par le lemme de Gauss et le raisonnement précédent, $p \mid p_{i_0}$. Comme on a déjà $p \mid q_{i_0}$, on voit que $p_{i_0} \wedge q_{i_0} \neq 1$, ce qui contredit l'hypothèse de 2.1. Ainsi, m et $c(mQ)$ sont effectivement premiers entre eux.

2.2 On a par hypothèse $P = QR$, donc $mm'P = (mQ)(m'R)$. On utilise alors le résultat de la section précédente : $mm'c(P) = c(mm'P) = c(mQ)c(m'R)$.

2.3 La relation précédente montre que m' divise $c(mQ)c(m'R)$. Comme m' et $c(m'R)$ sont premiers entre eux, le lemme de Gauss dit que m' divise $c(mQ)$. Ainsi, m' divise tous les coefficients de mQ et mQ/m' est bien à coefficients entiers. On montre de même que $m'R/m$ est à coefficients entiers.

2.4 Il est clair que, si P est le produit de deux polynômes non constants dans $\mathbf{Z}[X]$, c'est aussi le cas dans $\mathbf{Q}[X]$ car $\mathbf{Z} \subset \mathbf{Q}$. Réciproquement, si P s'écrit QR avec Q et R non constants à coefficents dans $\mathbf{Q}$, on en déduit comme ci-dessus deux polynômes non constants mQ/m' et $m'R/m$, à coefficients entiers, tels que $P = (mQ/m')(m'R/m)$.

3 Critère d'Eisenstein

3.1 Si $P = QR$ dans $\mathbf{Q}[X]$, il existe d'après la section précédente deux polynômes Q_1, R_1 de $\mathbf{Z}[X]$ tels que $P = Q_1R_1$. On remplace alors Q par Q_1 et R par R_1.

3.2 Pour tout polynôme $A = \sum \alpha_i X^i \in \mathbf{Z}[X]$, posons $\overline{A} = \sum \overline{\alpha_i} X^i$. L'application $\pi : \mathbf{Z}[X] \to \mathbf{F}_p[X],\ A \mapsto \overline{A}$ est un morphisme d'anneaux, et on a ainsi $\overline{P} = \overline{Q} \cdot \overline{R}$. Il suffit alors de remarquer que les hypothèses 1 et 2 de l'énoncé impliquent que $\overline{P} = \overline{a_n} X^n$.

3.3 On raisonne par l'absurde et on suppose que $\overline{Q} \neq \overline{b_q} X^q$ ou que $\overline{R} \neq \overline{c_r} X^r$. Alors $\overline{Q}$ ou $\overline{R}$ a un facteur irréductible différent de X. L'égalité $\overline{P} = \overline{Q} \cdot \overline{R}$ induit alors une décomposition de $\overline{P}$ différente de $\overline{a_n} X^n$, ce qui contredit l'unicité dans le théorème de décomposition en produit de facteurs irréductibles (théorème 5.6 p. 79 du cours).

3.4 La question précédente montre en particulier que $p \mid b_0$ et $p \mid c_0$. Ceci donne alors $p^2 \mid a_0 = b_0 c_0$, ce qui contredit précisément l'hypothèse 3 de l'énoncé. Ainsi, l'hypothèse de départ ($P = QR$, avec Q et R non constants) était fausse. Le polynôme P est donc irréductible dans $\mathbf{Q}[X]$.

3.5 Il suffit de remarquer que P satisfait les hypothèses du critère d'Eisenstein (hypothèses 1 à 3 de l'énoncé) pour $p = 5$.

4 Réduction modulo p

4.1 On écrit comme précédemment $Q = b_0 + \cdots + b_q X^q$ et $R = c_0 + \cdots + c_r X^r$. Il s'agit de montrer que $\overline{b_q}$ et $\overline{c_r}$ ne sont pas nuls. Mais si l'un d'eux l'était, on aurait $\overline{a_n} = \overline{b_q}\overline{c_r} = 0$, c'est-à-dire $p \mid a_n$, contrairement aux hypothèses. On a donc bien $\deg(\overline{Q}) = \deg Q = q$ et $\deg(\overline{R}) = \deg R = r$.

4.2 Comme $\overline{P} = \overline{Q} \cdot \overline{R}$ est supposé irréductible dans $\mathbf{F}_p[X]$, $\overline{Q}$ ou $\overline{R}$ est constant, c'est-à-dire qu'on a $\deg(\overline{Q}) = 0$ ou $\deg(\overline{R}) = 0$. Par la question précédente, on a ainsi $\deg(Q) = 0$ ou $\deg(R) = 0$, ce qui contredit l'hypothèse Q et R non constants et montre que P est irréductible dans $\mathbf{Q}[X]$.

4.3 On choisit $p = 2$. On a alors $\overline{P} = X^3 + X + 1$. Ce polynôme n'a pas de racines dans $\mathbf{F}_2$ (en effet, $\overline{P}(0) = \overline{P}(1) = 1$), et est de degré 3. Il est donc irréductible dans $\mathbf{F}_2[X]$. Ainsi, P vérifie les hypothèses du critère démontré ci-dessus pour $p = 2$: son coefficient dominant n'est pas divisible par 2, et $\overline{P}$ est irréductible. Donc P est irréductible dans $\mathbf{Q}[X]$.