Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Fiche TD 6

Exercice 1 *Intersection de courbes planes. Petit théorème de Bezout*
Soient P, Q dans $\mathbb{C}[X,Y]$ sans facteur commun. On veut montrer que l'ensemble des points d'intersection des deux courbes dans $\mathbb{C}^2$, d'équation respective $P(x,y)=0$, et $Q(x,y)=0$, est fini.

1. On considère P et Q dans $\mathbb{K}[Y]$, avec $\mathbb{K} := \mathbb{C}(X)$. Montrer que P et Q n'ont pas de facteur commun dans $\mathbb{K}[Y]$.
   Supposer que P et Q ont un facteur commun $R \in \mathbb{K}[Y]$, et poser $R = \frac{a}{b}R_0$, avec R_0 primitif (de contenu 1) dans $\mathbb{C}[X][Y]$. Montrer que R_0 divise P et Q dans $\mathbb{C}[X][Y]$.
2. Montrer qu'il existe deux polynômes U et V dans $\mathbb{C}[X,Y]$, et un polynôme non nul D de $\mathbb{C}[X]$ tels que $UP + VQ = D$.
   Commencer par appliquer l'identité de Bezout sur $\mathbb{K}[Y]$.
3. Conclure.
   Le polynôme D ne possède qu'un nombre fini de racines...

Exercice 2 *Théorème de décomposition en somme de deux carrés*
On veut montrer qu'un nombre premier impair p est somme de deux carrés (non nuls) si et seulement si p est congru à 1 modulo 4.

1. Constater ce théorème sur de petits nombres premiers.
2. Montrer l'implication.
   Regarder l'égalité $p = a^2 + b^2$ modulo p et montrer que -1 est alors un carré dans $\mathbb{F}_p$.
3. Montrer que p est si un premier congru à 1 modulo 4, p n'est pas irréductible dans $\mathbb{Z}[i]$.
   Considérer l'isomorphisme d'anneaux $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2+1)$.
4. Conclure.
   Décomposer $p = \alpha\beta$ dans $\mathbb{Z}[i]$, puis, calculer la norme de α.

Exercice 3 *Décomposition $p = s^2 + 3t^2$* On veut montrer qu'un nombre premier p (distinct de 3) s'écrit sous la forme $s^2 + 3t^2$ (avec s et t non nuls) si et seulement si p est congru à 1 modulo 3.

1. On suppose p premier distinct de 3. Montrer que -3 est un carré de $\mathbb{F}_p$ si et seulement si p est congru à 1 modulo 3.

   On peut commencer par remarquer que -3 est un carré modulo p si et seulement si X^3-1 possède une racine non triviale dans $\mathbb{F}_p$, et donc, si et seulement s'il existe un élément d'ordre 3 dans $\mathbb{F}_p$.

2. Conclure, en vous inspirant de l'exercice précédent.

   On pourra considérer l'anneau $\mathbb{Z}[j]$, qui est factoriel, et l'isomorphisme $\mathbb{Z}[j]/(p) \simeq \mathbb{F}_p[X]/(X^2+X+1)$.

Exercice 4 *Loi complémentaire de la réciprocité quadratique*

Soit $q = p^k$, avec p premier impair. Le but du problème est de prouver que 2 est un carré de $\mathbb{F}_q$ si et seulement si $q \equiv \pm 1$ modulo 8.

A. *Etude du polynôme X^4+1 sur $\mathbb{F}_q$*

Le but de cette partie est de montrer que le polynôme X^4+1 est toujours réductible sur $\mathbb{F}_q$. On considère une racine α de X^4+1 dans une extension de $\mathbb{F}_q$.

1. Montrer que X^4+1 ne possède pas de racine multiple (dans toute extension de $\mathbb{F}_q$).
2. Montrer que l'ensemble des racines de X^4+1 est $\{\alpha, -\alpha, \alpha^{-1}, -\alpha^{-1}\}$.

   Attention : la difficulté n'est pas de montrer qu'elles sont racines...
3. (a) Montrer que 8 divise l'ordre du groupe multiplicatif $\mathbb{F}_{q^2}^*$.

   Commencer par dire que $q^2-1 = (q-1)(q+1)$.

   (b) En déduire qu'il existe un élément α' d'ordre 8 dans $\mathbb{F}_{q^2}^*$.

   (c) Montrer alors que α' est racine de X^4+1.
4. En déduire que α est dans $\mathbb{F}_{q^2}$.
5. Conclure que X^4+1 est réductible sur $\mathbb{F}_q$.

B. *Implication « 2 est un carré de $\mathbb{F}_q \Longrightarrow q \equiv \pm 1$ modulo 8 »*

On considère encore une fois que α est une racine de X^4+1.

1. En remarquant que $\alpha^5 = -\alpha$, montrer que l'ensemble des racines de X^4+1 peut aussi s'écrire $\{\alpha, \alpha^3, \alpha^5, \alpha^{-1}\}$. En déduire que α^q ne peut être égal qu'à une de ces quatre valeurs.
2. Montrer que si $\alpha^q = \alpha^n$ pour un entier n, alors $q \equiv n$ modulo 8.
3. On pose maintenant $\beta = \alpha + \alpha^{-1}$. Montrer que $\beta^2 = 2$. Quelle est l'autre racine de $X^2 = 2$?
4. On suppose maintenant que 2 est un carré de $\mathbb{F}_q$. Montrer alors que $\beta^q = \beta$.
5. En déduire dans ce cas que $q \equiv \pm 1$ modulo 8.

C. *Implication « $q \equiv \pm 1$ modulo 8 $\Longrightarrow$ 2 est un carré de $\mathbb{F}_q$ »*

1. Montrer comment le raisonnement de la partie B s'inverse pour donner la réciproque.

2. En utilisant les notations standard du symbole de Legendre, montrer l'égalité suivante, où p désigne un nombre premier impair,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Exercice 5 *Le théorème de Chevalley-Warning*

Soit q une puissance d'un nombre premier p. On considère une famille de polynômes $P_1, \cdots, P_r$ dans $\mathbb{F}_q[X_1, \cdots, X_n]$, sans terme constant, et tels que $\sum_{i=1}^{r} \deg(P_i) < n$. Alors, il existe x non nul dans $V := \{x \in \mathbb{F}_q^n,\ P_i(x) = 0,\ \forall i\}$.

1. Soit $S_m := \sum_{y \in \mathbb{F}_q} y^m$. On suppose $m \geq 1$ et $q-1$ divise m. Montrer que $S_m = -1$.
   On utilise Lagrange qui assure que $y^m = 1$ dès que y est non nul.
2. On suppose $q-1$ ne divise pas m. Montrer que $S_m = 0$.
   Prendre un générateur z du groupe cyclique $\mathbb{F}_q^*$ et montrer que $z^m \neq 1$, puis, que $S_m = z^m S_m$.
3. Soit $P := \prod_{i=1}^{r}(1 - P_i^{q-1})$. Montrer que P est la fonction caractéristique de V, c'est-à-dire que $P(x)$ vaut 1 ou 0 selon si x est dans V ou non.
4. On considère $S_P := \sum_{x \in \mathbb{F}_q^n} P(x)$. Montrer que $S_P = |V|$ modulo p.
5. Montrer que le degré total t de P vérifie $t < (q-1)n$. On pose dans la suite $P = \sum_{m \in \mathbb{N}^n} c_m X_1^{m_1} \cdots X_n^{m_n}$, avec $\sum m_i < (q-1)n$.
6. Montrer que $S_P = \sum_{m \in \mathbb{N}^n} c_m S_{m_1} \cdots S_{m_n}$ et conclure.

Exercice 6 *Le théorème EGZ (Erdös-Ginzburg-Ziv)*

Soit p un nombre premier et a_i, $1 \leq i \leq 2p-1$ des entiers. Montrer que l'on peut extraire p entiers a_{i_k}, $1 \leq k \leq p$, parmi eux, tels que

$$a_{i_1} + a_{i_2} + \cdots + a_{i_p} \equiv 0 \pmod{p}.$$

Appliquer le théorème de Chevalley-Warning aux polynômes P_1 et P_2, avec

$$P_1 = \sum_{i=1}^{p} X_i^{p-1},\ P_2 = \sum_{i=1}^{p} a_i X_i^{p-1}.$$

On peut également montrer ce théorème pour p quelconque, non nécessairement premier.

Exercice 7 *(Non) Irréductibilité des polynômes cyclotomiques*

Soit n un entier positif et p et un nombre premier ne divisant pas n. On considère le polynôme cyclotomique $\phi_n \in \mathbb{Z}[X]$ et sa réduction $\overline{\phi}_n$ modulo p.

1. Soit $\mathbb{K}$ une extension de $\mathbb{F}_p$, montrer que l'application de $\mathbb{K}[X]$ dans lui même qui envoie $P = \sum_i a_i X^i$ sur $F(P) = \sum_i a_i^p X^i$, est un morphisme d'anneaux.
   On rappelle que le Frobenius $a \mapsto a^p$ est un automorphisme du corps $\mathbb{K}$.

2. Soit α une racine de $\overline{\phi}_n$ dans une extension de $\mathbb{F}_p$. Montrer que $\alpha^n = 1$.
   Décomposer $X^n - 1$ sur $\mathbb{Z}$ et quotienter par p.
3. Soit m l'ordre de p dans $\mathbb{Z}/n\mathbb{Z}^*$. Montrer que m est minimal non nul tel que $\alpha^{p^m} = 1$.
4. On considère le polynôme $Q = \prod_{k=0}^{m-1}(X - \alpha^{p^k})$. Montrer que $Q \in \mathbb{F}_p[X]$ et $Q(\alpha) = 0$.
   Pour la première assertion, on vérifiera que $F(Q) = Q$ en appliquant 1.
5. Montrer que si $m < \varphi(n)$, alors $\overline{\phi}_n$ n'est pas irréductible.
6. En déduire la propriété suivante : si $\mathbb{Z}/n\mathbb{Z}^*$ n'est pas cyclique, alors, pour tout p ne divisant pas n, $\overline{\phi}_n$ est réductible.

Exercice 8 *Exemple : réduction de ϕ_8*

On va montrer de façon constructive que $\phi_8 = X^4 + 1$, qui est irréductible sur $\mathbb{Z}$, est réductible modulo p, pour tout p premier. On notera au passage que cela provient (pour p impair) de l'exercice précédent et de l'isomorphisme $(\mathbb{Z}/8\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1. Montrer que ϕ_8 se réduit modulo 2.
2. On suppose maintenant p impair. Montrer que, soit $p \equiv 1$ [4], $p \equiv -1$ [8], soit $p \equiv 3$ [8]. Montrer que, dans le premier cas, -1 possède une racine carrée, disons $\beta \in \mathbb{F}_p$, dans le second cas, 2 possède une racine carrée, disons $\gamma \in \mathbb{F}_p$, dans le troisième cas, -2 possède une racine carrée, disons $\delta \in \mathbb{F}_p$.
   Utiliser le symbole de Legendre et la formule $\left(\begin{matrix}2\\p\end{matrix}\right) = (-1)^{\frac{p^2-1}{8}}$.
3. Soit α une racine de ϕ_8 dans une extension de $\mathbb{F}_p$. Montrer
$$X^4 + 1 = (X - \alpha)(X + \alpha)(X - \alpha^{-1})(X + \alpha^{-1}),$$
$$(\alpha + \alpha^{-1})^2 = 2, \text{ et } (\alpha - \alpha^{-1})^2 = -2.$$
4. On procède maintenant au cas par cas.
   (a) $p \equiv 1$ [4]. Montrer que $\phi_8 = (X^2 - \beta)(X^2 + \beta)$.
   (b) $p \equiv -1$ [8]. Montrer que $\phi_8 = (X^2 - \gamma X + 1)(X^2 + \gamma X + 1)$.
   (c) $p \equiv 3$ [8]. Montrer que $\phi_8 = (X^2 - \delta X - 1)(X^2 + \delta X - 1)$.