D. M. Agrégation Externe, le 16 octobre 2013

On rappelle le résultat suivant (formule des classes).

Soit $(G,\cdot)$ un groupe multiplicatif fini que l'on fait opérer sur lui même par conjugaison ($g\cdot h = ghg^{-1}$, pour $(g,h)\in G\times G$). En notant $G\cdot h_1,\cdots,G\cdot h_r$ toutes les orbites non réduites à un point et deux à deux distinctes, on a :

$$\operatorname{card}(G) = \operatorname{card}(Z(G)) + \sum_{i=1}^{r} \frac{\operatorname{card}(G)}{\operatorname{card}(G_{h_i})}$$

où $Z(G) = \{h\in G \mid \forall g\in G,\ gh=hg\}$ est le centre de G, $G\cdot h = \left\{ghg^{-1} \mid g\in G\right\}$ est l'orbite de h et $G_h = \left\{g\in G \mid ghg^{-1}=h\right\}$ le stabilisateur de h sous l'action de G.

Les anneaux considérés sont supposés unitaires et on notera respectivement $0_{\mathbb{A}}$, $1_{\mathbb{A}}$ (ou 0 et 1 quand l'anneau est fixé et qu'il n'y a pas d'ambiguïté) les éléments neutres pour l'addition et la multiplication d'un anneau $(\mathbb{A},+,\cdot)$, avec $0_{\mathbb{A}}\neq 1_{\mathbb{A}}$ (les anneaux considérés ont au moins deux éléments).

On note $\mathbb{A}^* = \mathbb{A}\setminus\{0_{\mathbb{A}}\}$, $\mathbb{A}^\times$ le groupe des éléments inversibles de $\mathbb{A}$ et :

$$Z(\mathbb{A}) = \{a\in\mathbb{A} \mid \forall b\in\mathbb{A},\ ab=ba\}$$

le centre de l'anneau $\mathbb{A}$.

On rappelle qu'un morphisme d'anneaux de $\mathbb{A}$ dans $\mathbb{B}$ (deux anneaux unitaires) est une application $\varphi:\mathbb{A}\to\mathbb{B}$ telle que $\varphi(1_{\mathbb{A}})=1_{\mathbb{B}}$ et :

$$\forall (x,y)\in\mathbb{A}^2,\ \varphi(x+y)=\varphi(x)+\varphi(y),\ \varphi(x\cdot y)=\varphi(x)\cdot\varphi(y)$$

Si $\mathbb{A}$ est un anneau commutatif, on note $\mathbb{A}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{A}$.

Soit $(\mathbb{K},+,\cdot)$ un corps. Le sous-corps premier de $\mathbb{K}$ est le sous-corps de $\mathbb{K}$ engendré par $1_{\mathbb{K}}$, c'est-à-dire l'intersection de tous les sous-corps de $\mathbb{K}$ (ou encore le plus petit sous-corps de $\mathbb{K}$).

Pour tout nombre premier $p\geq 2$, $\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ désigne le corps commutatif des classes résiduelles modulo p.

– I – Généralités

1. Soit $(\mathbb{A},+,\cdot)$ un anneau (unitaire). Montrer qu'il existe un unique morphisme d'anneaux $\varphi:\mathbb{Z}\to\mathbb{A}$.
2. Soit $(\mathbb{K},+,\cdot)$ un corps. Montrer que les seuls idéaux à gauche [resp. à droite] de $\mathbb{K}$ sont $\{0_{\mathbb{K}}\}$ et $\mathbb{K}$.
3. Soient $(\mathbb{K},+,\cdot)$ et $(\mathbb{L},+,\cdot)$ deux corps. Montrer qu'un morphisme de corps de $\mathbb{K}$ dans $\mathbb{L}$ est nécessairement injectif.
4. Montrer qu'un anneau unitaire intègre et fini est un corps.
5. Soit $(\mathbb{K},+,\cdot)$ un corps. Montrer que son sous-corps premier est soit infini isomorphe à $\mathbb{Q}$, soit fini isomorphe à $\mathbb{Z}_p$, où $p\geq 2$ est un nombre premier.
   Dans le cas où $\mathbb{K}$ est fini, montrer qu'il existe un nombre premier $p\geq 2$ et un entier $n\geq 1$ tels que $\operatorname{card}(\mathbb{K}) = p^n$.
   Dans le premier cas, on dit que $\mathbb{K}$ est de caractéristique nulle et dans le second qu'il est de caractéristique p. Précisément, en désignant par $\varphi:\mathbb{Z}\to\mathbb{K}$ le morphisme d'anneaux défini par :
   $$\forall n\in\mathbb{Z},\ \varphi(n) = n\cdot 1_{\mathbb{K}}$$
   on a $\ker(\varphi) = p\mathbb{Z}$, où p est la caractéristique de $\mathbb{K}$.
6. Soient $\mathbb{K}\subset\mathbb{L}$ deux corps. Montrer qu'ils sont de même caractéristique.
7. Soient $\mathbb{K}$ un corps de caractéristique $p\geq 2$ et $\mathbb{A}$ une $\mathbb{K}$-algèbre. Montrer que pour tous a,b dans $\mathbb{A}$ qui commutent, on a :
   $$(a+b)^p = a^p + b^p$$
8. Soient $(\mathbb{K},+,\cdot)$ un corps commutatif, $m\geq n$ deux entiers naturels non nuls et q,r le quotient et le reste dans la division euclidienne de m par n.
   (a) Déterminer le quotient et le reste quand on effectue la division euclidienne de X^m-1 par X^n-1 dans $\mathbb{K}[X]$.
   (b) Donner une condition nécessaire et suffisant pour que X^n-1 divise X^m-1 dans $\mathbb{K}[X]$.
   (c) Soit $q\geq 2$ un entier. Montrer que q^n-1 divise q^m-1 dans $\mathbb{Z}$ si, et seulement si, n divise m.
   (d) Montrer que $(X^n-1)\wedge(X^m-1) = X^{n\wedge m}-1$ dans $\mathbb{K}[X]$.
9. Soient $\mathbb{K}\subset\mathbb{L}$ deux corps et P,Q dans $\mathbb{K}[X]$. Expliquer pourquoi les pgcd (unitaires) de P et Q dans $\mathbb{K}[X]$ et $\mathbb{L}[X]$ sont identiques.

10. Si $P(X)=\sum_{k=0}^{n} a_k X^k$ est un polynôme non nul à coefficients entiers relatifs, on définit son contenu par :

$$c(P)=\operatorname{pgcd}(a_0,a_1,\cdots,a_n).$$

On dit que $P\in\mathbb{Z}[X]\setminus\{0\}$ est primitif si son contenu vaut 1.

(a) Montrer que le produit de deux polynômes primitifs dans $\mathbb{Z}[X]$ est primitif.

(b) Montrer que si P et Q sont deux polynômes non nuls dans $\mathbb{Z}[X]$ alors $c(PQ)=c(P)\,c(Q)$ (lemme de Gauss).

11. Montrer que si P est un polynôme unitaire de $\mathbb{Z}[X]$ tel que $P=QR$ avec Q,R dans $\mathbb{Q}[X]$ et Q unitaire, alors Q et R sont dans $\mathbb{Z}[X]$.
12. Soit P un polynôme unitaire de $\mathbb{Z}[X]$. Montrer qu'il existe des polynômes $P_1,\cdots,P_r$ unitaires dans $\mathbb{Z}[X]$ et irréductibles dans $\mathbb{Q}[X]$ tels que $P=\prod_{k=1}^{r} P_k$.
13. Soit p un nombre premier. À tout polynôme $P(X)=\sum_{k=0}^{p} a_k X^k$ dans $\mathbb{Z}[X]$, on associe le polynôme $\overline{P}(X)=\sum_{k=0}^{p}\overline{a_k}X^k$ dans $\mathbb{Z}_p[X]$, où $\overline{a}$ désigne la classe de $a\in\mathbb{Z}$ dans $\mathbb{Z}_p$ (l'application $P\mapsto\overline{P}$ est un morphisme d'anneaux surjectif).
Montrer que pour tout polynôme $Q\in\mathbb{Z}[X]$, on a $\overline{Q^p}(X)=\overline{Q}(X^p)$.
14. Soient $n\in\mathbb{N}^*$ et p un nombre premier qui ne divise pas n. Montrer que dans $\mathbb{Z}_p[X]$, le polynôme $X^n-\overline{1}$ est sans facteur carré (i. e. ne peut s'écrire Q^2R avec Q non constant).

– II – Polynômes cyclotomiques

Pour tout entier naturel non nul n, on note :
- $\mathcal{D}_n$ l'ensemble des diviseurs positifs de n ;
- ω_n le nombre complexe $\exp\left(\dfrac{2i\pi}{n}\right)$;
- Γ_n le sous-groupe multiplicatif de $\mathbb{C}^*$ formé de l'ensemble des racines n-ème de l'unité, soit :

$$\Gamma_n=\{z\in\mathbb{C}\mid z^n=1\}=\left\{\omega_n^k\mid 1\leq k\leq n\right\}$$

- $\mathcal{P}_n$ l'ensemble des générateurs du groupe multiplicatif Γ_n, soit $\mathcal{P}_1=\Gamma_1$ et pour $n\geq 2$:

$$\begin{aligned}\mathcal{P}_n&=\left\{z\in\Gamma_n\mid z^n=1 \text{ et } z^k\neq 1 \text{ pour } 1\leq k\leq n-1\right\}\\&=\left\{\omega_n^k\mid 1\leq k\leq n \text{ et } k\wedge n=1\right\}\end{aligned}$$

(les éléments de $\mathcal{P}_n$ sont les racines primitives n-ème de l'unité) ;
- Φ_n le n-ème polynôme cyclotomique défini par :

$$\Phi_n(X)=\prod_{\omega\in\mathcal{P}_n}(X-\omega)=\prod_{\substack{k=1\\ k\wedge n=1}}^{n}\left(X-\omega_n^k\right)$$

On suppose connue la fonction indicatrice d'Euler :

$$\varphi:n\in\mathbb{N}^*\mapsto\varphi(n)=\operatorname{card}\left(\mathbb{Z}_n^{\times}\right)=\operatorname{card}\{k\in\{1,\cdots,n\}\mid k\wedge n=1\}$$

1. Quel est le degré de Φ_n pour $n\geq 1$.
2. Montrer que pour tout nombre premier $p\geq 2$, on a :

$$\Phi_p(X)=\sum_{k=0}^{p-1}X^k$$

3. Montrer que, pour tout $n\in\mathbb{N}^*$, on a la partition :

$$\Gamma_n=\bigcup_{d\in\mathcal{D}_n}\mathcal{P}_d$$

4. Montrer que, pour tout $n \in \mathbb{N}^*$, on a :
$$X^n - 1 = \prod_{d \in \mathcal{D}_n} \Phi_d(X)$$
et en déduire la formule de Möbius :
$$\forall n \geq 1,\ n = \sum_{d \in \mathcal{D}_n} \varphi(d)$$

5. Montrer que pour tout $n \geq 1$, Φ_n est unitaire et dans $\mathbb{Z}[X]$ et calculer $\Phi_n(0)$.

6. On se propose de montrer que, pour tout $n \geq 2$, le polynôme Φ_n est irréductible dans $\mathbb{Q}[X]$ (pour $n = 1$, il est clair que $\Phi_1(X) = X - 1$ est irréductible).
D'après **I.12.** il existe des polynômes $P_1, \cdots, P_r$ unitaires dans $\mathbb{Z}[X]$ et irréductibles dans $\mathbb{Q}[X]$ tels que $\Phi_n = \prod_{k=1}^{r} P_k$ (la question **II.5** nous dit que Φ_n est unitaire et dans $\mathbb{Z}[X]$).

   (a) Soient ζ une racine complexe de P_1 et $p \geq 2$ un nombre premier ne divisant pas n.

      i. Montrer qu'il existe un indice k compris entre 1 et r tel que $P_k(\zeta^p) = 0$.

      ii. Montrer que $k = 1$.

   (b) Montrer que $P_1\left(\omega_n^k\right) = 0$ pour tout entier k premier avec n et conclure.

7. On dit qu'un nombre complexe α est algébrique s'il existe un polynôme non nul P dans $\mathbb{Q}[X]$ tel que $P(\alpha) = 0$.
Soit α un nombre algébrique.

   (a) Montrer qu'il existe un unique polynôme unitaire P_α dans $\mathbb{Q}[X]$ tel que :
$$\mathcal{I}_\alpha = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\} = \mathbb{Q}[X] \cdot P_\alpha.$$
   On dit que P_α est le polynôme minimal de α.

   (b) Montrer que le polynôme minimal de α est l'unique polynôme unitaire irréductible de $\mathbb{Q}[X]$ qui annule α.

8. Montrer que, pour $n \in \mathbb{N}^*$ et tout entier k compris entre 1 et n premier avec n, ω_n^k est algébrique et que son polynôme minimal est Φ_n.

– III – Un cas particulier du théorème de Dirichlet

On se propose de montrer le cas particulier suivant du théorème de Dirichlet : pour tout entier $n \geq 1$, il existe une infinité de nombres premiers de la forme $1 + kn$ où $k \in \mathbb{N}^*$.

1. Soient $n \in \mathbb{N}^*$, $a \in \mathbb{Z}$ et $p \geq 2$ un nombre premier.
Montrer que si p divise $\Phi_n(a)$ et ne divise aucun des $\Phi_d(a)$ pour $d \in \mathcal{D}_n \setminus \{n\}$, alors p est congru à 1 modulo n.
2. Montrer que pour tout $n \geq 2$ et tout entier $a \geq 2$, on a $|\Phi_n(a)| > a - 1$.
3. Soient $n \in \mathbb{N}^*$, $m \geq n + 2$ un entier, $a = m!$ et $p \geq 2$ un diviseur premier de $\Phi_n(a)$ (il en existe puisque $a \geq 3$ entraîne $|\Phi_n(a)| > a - 1 \geq 2$ pour $n \geq 2$ et $\Phi_1(a) = a - 1 \geq 2$).

   (a) Montrer que $p > m$.

   (b) Montrer que p ne divise aucun des $\Phi_d(a)$ pour $d \in \mathcal{D}_n \setminus \{n\}$ et conclure.

– IV – Un théorème de Jacobson

Le but de cette partie est de montrer le résultat suivant.

Théorème 1 *Si $(\mathbb{A}, +, \cdot)$ est un anneau unitaire tel que :*
$$\forall a \in \mathbb{A},\ \exists n \in \mathbb{N} \setminus \{0, 1\} \mid a^n = a \tag{1}$$
alors $\mathbb{A}$ est commutatif.

On désigne par $(\mathbb{A}, +, \cdot)$ un anneau (unitaire).
On rappelle qu'un élément a de $\mathbb{A}$ est dit :
– nilpotent s'il existe un entier $r \in \mathbb{N}^*$ tel que $a^r = 0_\mathbb{A}$;
– idempotent si $a^2 = a$.

1. On suppose que :
$$\forall a \in \mathbb{A},\ a^2 = a$$
(on dit que $\mathbb{A}$ est un anneau de Boole). Montrer que $\mathbb{A}$ est commutatif de caractéristique égale à 2.
Dans ce qui suit, $\mathbb{A}$ est un anneau (unitaire) vérifiant la condition (1).
Pour tout $a \in \mathbb{A}$, on désigne par n_a le plus petit entier de $\mathbb{N} \setminus \{0,1\}$ tel que $a^{n_a} = a$ et on note $\gamma_a = a^{n_a - 1}$.

2.
   (a) Montrer que :
$$\forall a \in \mathbb{A},\ \forall n \in \mathbb{N}^*,\ a^n \in \left\{a, \cdots, a^{n_a - 1}\right\}.$$
   (b) Déterminer les éléments nilpotents de $\mathbb{A}$.
   (c) Montrer que :
$$\forall (a,b) \in \mathbb{A}^2,\ (ab = 0_{\mathbb{A}} \Leftrightarrow ba = 0_{\mathbb{A}})$$
   (d) Montrer que tout élément idempotent de $\mathbb{A}$ est dans le centre $Z(\mathbb{A})$.
   (e) Montrer que pour tout $a \in \mathbb{A}$, γ_a est idempotent et dans $Z(\mathbb{A})$.

À tout élément a de $\mathbb{A}$, on associe l'entier :
$$m_a = (n_a - 1)(n_{2a} - 1) + 1$$

3. Montrer que, pour tout $a \in \mathbb{A}$, on a :
$$a^{m_a} = a,\ (2a)^{m_a} = 2a,\ (2^{m_a} - 2)\, a = 0_{\mathbb{A}}$$

4. On suppose, seulement pour cette question, que :
$$\forall a \in \mathbb{A},\ a^3 = a$$
Montrer que $\mathbb{A}$ est commutatif.
À tout $a \in \mathbb{A}^*$, on associe l'ensemble :
$$\mathbb{P}(a) = \{y \in \mathbb{A} \mid \exists P \in \mathbb{Z}[X] \text{ tel que } y = aP(a)\}$$

5. Soit $a \in \mathbb{A}^*$.
   (a) Montrer que $\mathbb{P}(a)$ est un sous-anneau commutatif fini de $\mathbb{A}$ et que :
$$\mathbb{P}(a) = \left\{ \sum_{k=1}^{n_a - 1} \alpha_k a^k \mid \alpha_k \in \{0, \cdots, 2^{m_a} - 3\} \right\}$$
   (b) Montrer que γ_a est l'élément neutre de $\mathbb{P}(a)$, c'est-à-dire que :
$$\forall y \in \mathbb{P}(a),\ \gamma_a \cdot y = y$$
   et que a est inversible dans $\mathbb{P}(a)$.
   (c) Montrer que pour tout $x \in \mathbb{A}^*$ idempotent, l'application $\varphi_x : y \mapsto xy$ est un morphisme d'anneaux (unitaires) surjectif de $\mathbb{P}(a)$ sur $\mathbb{P}(xa)$.

6. On suppose que l'anneau $\mathbb{A}$ est non commutatif et pour $a \in \mathbb{A}^*$, on désigne par $E_a = (\mathbb{P}(a))^* \setminus (\mathbb{P}(a))^\times$ l'ensemble des éléments non inversibles de $(\mathbb{P}(a))^*$.
On se donne $a \in \mathbb{A} \setminus Z(\mathbb{A})$ et $b \in \mathbb{A}$ tel que $c = ba - ab \neq 0_{\mathbb{A}}$.
   (a) Montrer que $\gamma_c a \in \mathbb{A} \setminus Z(\mathbb{A})$.
   (b) On suppose que $\mathbb{P}(a)$ n'est pas un corps et on se donne $x \in E_a$.
   Montrer que si $\gamma_c x = 0_{\mathbb{A}}$, alors $\mathbb{P}(\gamma_c a)$ a strictement moins d'éléments non inversibles que $\mathbb{P}(a)$, sinon $\gamma_x a \in \mathbb{A} \setminus Z(\mathbb{A})$ et $\mathbb{P}(\gamma_x a)$ a strictement moins d'éléments non inversibles que $\mathbb{P}(a)$.
   (c) Montrer qu'il existe un élément $a \in \mathbb{A} \setminus Z(\mathbb{A})$ tel que $\mathbb{P}(a)$ soit un corps.

7. Soit $\mathbb{K}$ un corps fini (donc commutatif) de caractéristique $p \geq 2$ et de cardinal $q = p^n$ (avec $n \geq 1$) contenu dans $\mathbb{A}$. L'anneau $\mathbb{A}$ peut alors être muni d'une structure de $\mathbb{K}$-espace vectoriel.
À tout élément x de $\mathbb{K}$, on associe l'application :
$$\begin{array}{cccc} \delta_x & \mathbb{A} & \to & \mathbb{A} \\ & y & \mapsto & yx - xy \end{array}$$

(a) Montrer que, pour tout x dans $\mathbb{K}$, l'application δ_x est linéaire.

(b) Montrer que, pour tout x dans $\mathbb{K}$ et tout entier $m \geq 1$, on a :

$$\forall y \in \mathbb{A},\ \delta_x^m(y) = \sum_{k=0}^{m} (-1)^k C_m^k x^k y x^{m-k}$$

où $\delta_x^m = \underbrace{\delta_x \circ \cdots \circ \delta_x}_{m \text{ fois}}$.

(c) Montrer que, pour tout x dans $\mathbb{K}$ et tout entier $r \geq 1$, on a $\delta_x^{p^r} = \delta_{x^{p^r}}$, puis que $\delta_x^q = \delta_x$.

(d) Montrer que, pour tout x dans $\mathbb{K}$, on a :

$$\mathbb{A} = \bigoplus_{\lambda \in \mathbb{K}} \ker(\delta_x - \lambda Id_{\mathbb{A}})$$

(e) Montrer que si $x \in \mathbb{K}$ et $x \notin Z(\mathbb{A})$, il existe alors $\lambda \in \mathbb{K}$ et $y \in \mathbb{A}$ tels que $\delta_x(y) = \lambda y \neq 0_{\mathbb{A}}$.

8. On suppose que l'anneau $\mathbb{A}$ est non commutatif et on se donne $a \in \mathbb{A} \setminus Z(\mathbb{A})$ tel que $\mathbb{P}(a)$ soit un corps (question **V.6c**). Il existe alors $\lambda \in \mathbb{P}(a)$ et $b \in \mathbb{A}^*$ tel que $\lambda b = \delta_a(b) \neq 0_{\mathbb{A}}$, ce qui peut aussi s'écrire $ba = \mu b \neq ab$ avec $\mu = \lambda + a \in \mathbb{P}(a)$. On associe alors à ces éléments a, b l'ensemble :

$$\mathbb{P}(a,b) = \left\{ \sum_{\substack{1 \leq k \leq n \\ 1 \leq j \leq m}} \alpha_{k,j} a^k b^j \mid (n,m) \in \mathbb{N}^* \text{ et } \alpha_{k,j} \in \mathbb{Z} \right\}$$

(a) Montrer que pour tout $j \in \mathbb{N}^*$ et tout $y \in \mathbb{P}(a)$, il existe un élément $z \in \mathbb{P}(a)$ tel que $b^j y = z b^j$.

(b) Montrer que :

$$\mathbb{P}(a,b) = \left\{ \sum_{\substack{1 \leq k \leq n_a - 1 \\ 1 \leq j \leq n_b - 1}} \alpha_{k,j} a^k b^j \mid \alpha_{k,j} \in \{0, \cdots, 2^{m_a} - 3\} \right\}$$

et que $\mathbb{P}(a,b)$ est un sous-anneau fini non commutatif de $\mathbb{A}$ d'élément neutre $\gamma_a \gamma_b$.

(c) Montrer qu'il existe $a \in \mathbb{A} \setminus Z(\mathbb{A})$, $b \in \mathbb{A}^*$ et $\mu \in \mathbb{P}(a)$ tels que $ba = \mu b \neq ab$ et $\mathbb{P}(a,b)$ soit un corps.

(d) En déduire le théorème de Jacobson.