Sommaire

1 Théorie des groupes

1.1 Exemples de sous-groupes

1. Montrer que, pour tout $a \in \mathbb{R}$, l'ensemble $a\mathbb{Z} = \{am : m \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{R}, +)$.
2. Montrer que $\mathbb{U}_n$ (l'ensemble des racines n-ème de l'unité) est un sous-groupe de $\mathbb{U}$ (l'ensemble des nombres complexes de module 1 muni du produit).
3. Montrer que $\cup_{n\in\mathbb{N}}\mathbb{U}_n$ est un sous-groupe strict de $\mathbb{U}$.
4. (*) Soit p un nombre premier. Construire un p-groupe infini, c'est-à-dire un groupe dont tous les éléments sont d'ordre une puissance de p.

   On pourra s'aider des racines de l'unité.

1.2 Exemples de sous-groupes normaux

Soit G un groupe. On note $Z(G)$ le centre de G défini par

$$Z(G) = \{x \in G : \forall g \in g, \quad xg = gx\}$$

et $D(G)$ le groupe engendré par les commutateurs, i.e. $D(G)$ est le sous-groupe de G engendré par les $[g, h] = ghg^{-1}h^{-1}$ où $g, h \in G$.

1. Montrer que $Z(G)$ et $D(G)$ sont des sous-groupes normaux de G.
2. Montrer que l'on a $G/Z(G) \simeq \mathrm{Int}(G)$ où $\mathrm{Int}(G)$ désigne le groupe des automorphismes de G intérieurs, c'est-à-dire ceux de la forme

   $$g \mapsto xgx^{-1}.$$

3. Montrer que $G/D(G)$ est abélien et que si H est un sous-groupe normal de G tel que G/H est abélien, alors on a $D(G) \subset H$.

   En ce sens, on retiendra que $G/D(G)$ est le plus grand quotient abélien de G.

1.3 Groupe abélien

1. Soit G un groupe tel que $G/Z(G)$ est cyclique. Montrer que G est abélien.

   De sorte qu'en fait $G/Z(G)$ est trivial.

2. Soien p un nombre premier et G est un groupe d'ordre p^2. Montrer que G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}^2$.

1.4 Le carré est trivial

Soit G un groupe tel que

$$\forall g \in G, \quad g^2 = 1.$$

1. Montrer que G est commutatif.

   On pourra observer que $g = g^{-1}$ pour tout $g \in G$.

2. Montrer qu'un tel groupe peut être vu comme $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel.

   On pourra poser $\lambda.g = g^{\lambda}$.

3. Réciproquement, montrer qu'un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel est en fait un groupe qui satisfait la condition de l'énoncé.

1.5 Nombre fini de sous-groupes

Caractériser les groupes n'ayant qu'un nombre fini de sous-groupes.

1.6 Théorème de Cayley

Soit G un groupe (fini). Montrer que G s'identifie à un sous-groupe de S_G (le groupe des permutations de G) via

$$\gamma : \left| \begin{array}{ccc} G & \longrightarrow & S_G \\ g & \longmapsto & (x \in G \mapsto xg) \end{array} \right. .$$

1.7 Sous-groupes de $(\mathbb{R}, +)$ (*)

Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$.

1. Montrer que l'ensemble $G \cap \mathbb{R}_+^*$ est non vide et justifier l'existence de $a = \inf(G \cap \mathbb{R}_+^*)$.
2. On suppose ici que l'on a $a > 0$.
   (a) Montrer que l'on a $a \in G$ puis que $a\mathbb{Z}$ est inclus dans G.
   (b) Soit $x \in G$. Justifier qu'il existe $n \in \mathbb{Z}$ tel que $x - na \in [0, a[$ puis montrer que ce réel est nul.
   (c) Conclure.
3. On suppose maintenant que l'on a $a = 0$. Montrer que G est dense dans $\mathbb{R}$.

   Pour $\varepsilon > 0$, on pourra réaliser la division euclidienne d'un réel x par $g \in G \cap]0, \varepsilon[$.

4. *Applications*
   (a) Soit $f : \mathbb{R} \to \mathbb{R}$ périodique continue non constante. Montrer que f admet une plus petite période strictement positive.
   (b) Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Montrer que $\mathbb{Z} + \alpha\mathbb{Z}$ est dense dans $\mathbb{R}$.
   (c) (*) Montrer que $\cos(\mathbb{N})$ est dense dans $[-1; 1]$.

1.8 Groupe d'automorphisme trivial (*)

Que dire d'un groupe $(G, .)$ dont le groupe des automorphismes est réduit à Id_G?

On pourra chercher à construire un automorphisme de G a priori non trivial pour commencer à tirer de l'information.

Solution: Le groupe des automorphismes intérieurs est en particulier lui aussi trivial, de sorte que G est abélien. Alors, l'application $g \mapsto g^{-1}$ est un automorphisme de G; par hypothèse, il est donc trivial, c'est-à-dire que l'on a $g^2 = 1$ (si l'on garde la notation multiplicative) pour tout $g \in G$. Ainsi, G est un $\mathbb{F}_2$-espace vectoriel et en se servant d'une base de G, on peut construire un automorphisme de G non trivial dès que G est d'ordre plus grand que 4.

1.9 Groupe d'automorphisme cyclique (Eloan Rapion) (*)

Soit $p \geq 3$ un nombre premier. Montrer qu'il n'existe pas de groupe G tel que $Aut(G) \simeq \mathbb{Z}/p\mathbb{Z}$.

Solution: On a G abélien puisque $G/Z(G) \simeq Int(G) \leqslant Aut(G) \simeq \mathbb{Z}/p\mathbb{Z}$. Alors, $x \mapsto x^{-1}$ est soit un élément d'ordre 2, soit l'identité. Ca ne peut pas être un élément d'ordre 2 sans quoi on aurait $2|p$. C'est donc l'identité i.e. on a $x^2 = 1$ pour tout $x \in G$. Alors, G est un $\mathbb{Z}/2\mathbb{Z}$-ev et on vérifie facilement que $Aut(G) = GL_{dim(G)}(\mathbb{F}_2)$ qui n'est jamais premier.

1.10 Autour des groupes de Prüfer (Eloan Rapion) (**)

1. Décrire les groupes infini G dont l'ensemble des sous-groupes est totalement ordonné (pour l'inclusion). Que dire si G est fini ?
2. Décrire les groupes abéliens infinis G dont l'intersection de tous les sous-groupes non nuls soit non triviale.
3. Décrire les groupes abéliens infinis G dont les sous-groupes stricts sont tous finis.

Solution:

1. Déjà, on peut remarquer qu'étant donné $a, b \in G$, on a par hypothèse $< a > \subset < b >$ ou l'inverse, i.e. a est une puissance de b ou l'inverse, ce à quoi on fera référence par "le fait clé".

   Ensuite, tout $g \in G$ est d'ordre fini puisque $< g^2 > \subset < g^3 >$ donne un $k \in \mathbb{Z}$ tel que $g^{2-3k} = 1$ et on a $2 - 3k! = 0$ (on a quelque chose de similaire si l'on suppose $< g^3 > \subset < g^2 >$).

   De plus, cet ordre est la puissance d'un nombre premier, sans quoi, en notant $p^a q^b m$ sont ordre (sous les hypothèses évidentes $a, b > 0$, $p, q \in \mathbb{P}$, $p \neq q$, $p, q \not| m$), les sous-groupes $< g^{p^a} >$ et $< g^{q^b} >$ (à cause du fait clé et du fait que g^{p^a} a un ordre premier avec p, g^{q^b} premier avec q).

   En fait, on peut (maintenant) même dire qu'il existe $p \in \mathbb{P}$ tel que tout $g \in G$ soit d'ordre une puissance de p à cause de ce qui précède et du fait clé.

   Aussi, pour tout $k \in \mathbb{N}$, il existe au plus un sous-groupe de G d'ordre p^k car, si H_1 et H_2 sont deux tels sous-groupes, on a, par hypothèse, $H_1 \subset H_2$ ou l'inverse, puis égalité par cardinalité.

Alors, il y a une infinité de tel k, sans quoi G serait fini puisque tout $g \in G$ appartient à $< g >$, qui est un sous-groupe d'ordre $p^{o(g)}$. En fait, à cause du théorème de structure, on peut même dire que tout sous-groupe d'ordre p^k est engendré par un seul élément (sinon, toute pseudo-base de ce sous-groupe est de cardinal supérieur à 2 et donc on a en particulier deux éléments distincts qui constituent cette pseudo base engendrent des groupes qui sont incomparables).

Par conséquent, cette infinité de k est en fait $\mathbb{N}$ tout entier. On peut donc écrire $G = \bigcup_{k\in\mathbb{N}} G_{p^k}$ où G_{p^k} est le sous-groupe de G d'ordre p^k.

Finalement, on constate qu'à isomorphisme près, les seuls groupes possibles sont les $\bigcup_{k\in\mathbb{N}} \mathbb{U}_{p^k}$ où $p \in \mathbb{P}$. On peut expliciter un isomorphisme entre $G = \bigcup_{k\in\mathbb{N}} G_{p^k}$ et $\bigcup_{k\in\mathbb{N}} \mathbb{U}_{p^k}$ où $p \in \mathbb{P}$ en notant $a_1 \in G$ un élément d'ordre p et en construisant par récurrence a_k comme racine p^e de a_{k-1} dans G. Il suffit maintenant de constater que

$$g \in G \mapsto exp(\frac{2i\pi k}{p^n}) \text{ si } g = a_n^k$$

est bien définie et définit effectivement un isomorphisme comme celui recherché.

Si G est fini, on montre que G est cyclique d'ordre une puissance d'un nombre premier et que cela est une condition suffisante.

2. Tout d'abord, tout $g \in G$ est d'ordre fini puisque $\bigcap_{n\in\mathbb{N}^*} n\mathbb{Z} = 0$.

   Ensuite, puisque les p-Sylow de G, notés S_p, sont d'intersection triviale, il existe $p \in \mathbb{P}$ tel que $G = S_p$ (un p-Sylow est non-trivial à partir du moment où il existe un élément dont l'ordre est divisible par p).

   Aussi, il n'existe qu'un seul sous-groupe d'ordre p puisque si l'on se donne deux tels sous-groupes H_1, H_2, ils sont forcément cycliques, engendrés respectivement par des certains a_1, a_2. Alors, l'hypothèse $H_1 \cap H_2 \neq \{1\}$ donne $0 < j, k < p$ tels que $a_1^k = a_2^j$. Puisque l'on a $0 < k < p$, on a $k \wedge p = 1$, si bien qu'un couple de Bézout (u, v) associé (k, p) donne $a_1 = a_1^{ku} = a_2^{ju}$. On en déduit $H_1 =< a_1 > \subset < a_2 >= H_2$, puis l'égalité cherchée par cardinalité.

   Remarquons également que tout sous-groupe fini est forcément cyclique à cause du théorème de structure.

   Tâchons maintenant de montrer que tout élément admet une racine p^e. On note f le morphisme "puissance p" (qui est bien un morphisme car G est abélien). On veut donc montrer que l'on a $Im(f) = G$. Par l'absurde, supposons qu'il existe $a \notin Im(f)$. Soit $b \in G$. Par ce qui précède, il existe $c \in G$ tel que $< a, b >=< c >$. Il s'ensuit qu'il existe $k \in \mathbb{Z}$ tel que $a = c^k$ et on a $p \wedge k = 1$ puisque $a \notin Im(f)$. Ainsi, en utilisant l'astuce précédent avec le couple de Bézout, on trouve que l'on a $c \in < a >$ et de l'égalité $< a, b >=< c >$ on tire maintenant $b \in < a >$. On obtient finalement $G =< a >$, ce qui est absurde puisque G est infini et que a est d'ordre fini.

On peut donc construire une suite $(a_n) \in G^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, a_n est d'ordre p^n et $a_{n+1}^p = a_n$. Montrons que l'on a $G =< a_n >_{n\in\mathbb{N}}$. Soit $b \in G$. On considère le plus petit $j \in \mathbb{N}^*$ tel que $b^j \in < a_n >_{n\in\mathbb{N}}$ (qui n'est rien d'autre que l'ordre de b dans le groupe quotient). Remarquons que l'on a $< a_n >_{n\in\mathbb{N}} = \bigcup_{n\in\mathbb{N}} < a_n >$. Distinguons deux cas : soit $j \wedge p = 1$, dans quel cas l'astuce avec le couple de Bézout donne $b \in < a_n >_{n\in\mathbb{N}}$, soit $p \mid j$, si bien que l'on peut écrire $b^{pj'} = a_n^k = a_{n+1}^{pk}$ pour des certains n, k (on pose $j = pj'$). Ainsi, on a $(b^{j'} a_{n+1}^{-k})^p = 1$ si bien que $b^{j'} a_{n+1}^{-k}$ est d'ordre 1 ou p, i.e. cet élément appartient à l'unique sous-groupe d'ordre p, qui n'est autre que $< a_1 >$. Ainsi, on a $b^{j'} \in < a_{n+1}$ et le fait que $j' < j$ viennent contredire la définition de j. Autrement dit, le deuxième cas traité ici n'arrive jamais.

Finalement, on a bien l'égalité annoncé et on conclut comme en q.1.

3. Tout d'abord, tout $g \in G$ est d'ordre fini sinon deux cas se dessinent : soit $< g >$ est un sous-groupe strict (infini) - ce qui contredit l'hypothèse faite sur G - soit $< g >= G$, si bien que $< g^2 >$ est un sous-groupe strict infini - ce qui contredit de nouveau l'hypothèse faite sur G.

   De plus, il existe au plus un $p \in \mathbb{P}$ tel que le p-Sylow S_p (il n'en existe qu'un seul car G est abélien, il s'agit du sous-groupe formé par l'ensemble des éléments d'ordre $p^?$) de G soit de cardinal infini puisque l'on aurait $G = S_p$ (pousser le raisonnement un cheveux plus loin n'est pas compliqué).

   Tâchons de montrer qu'il en existe bien un en raisonnant par l'absurde. Supposons donc que S_p soit fini pour tout $p \in \mathbb{P}$. Alors, puisque G est produit de ses p-Sylow, on peut affirmer que $A = \{p \in \mathbb{P} : |S_p| \neq 1\}$ est infini, sans quoi G serait fini. Ainsi, en fixant $p_0 \in A$ quelconque, on aboutit à l'absurdité que le produit des S_p pour tout $p \neq p_0$ est un sous-groupe strict infini de G.

   Ainsi, on a un (unique) $p \in \mathbb{P}$ tel que $G = S_p$.

   Montrons maintenant que tout élément de G admet une racine p^e. Pour cela, remarquons d'abord qu'il n'y a qu'un nombre fini d'éléments d'ordre p. Par l'absurde, si ce n'était pas le cas, on pourrait construire une suite $(g_n) \in G^{\mathbb{N}}$ telle que, pour tout $n \geq 0$, g_n est d'ordre p et $g_n \notin < g_0, ..., g_{n-1} >$. On aurait alors $G =< g_n >_{n\in\mathbb{N}} =< g_1, ... >$ d'où $g_0 = g_1^{i_1} \cdots g_m^{i_m}$ avec $0 < i_m < p$, si bien que l'on aurait $i_m \wedge p = 1$ puis en choisissant un couple de Bézout (u, v) associé, on aurait $g_0^u g_1^{-i_1 u} \cdots g_{m-1}^{-i_{m-1} u} = g_m$, ce qui contredit la construction de (g_n).

   On peut maintenant démontrer ce que l'on a annoncé plus haut. Pour cela, on considère $X = \{g \in G : \exists x \in G \quad x^p = g\} = Im(f)$ où f est le morphisme "puissance p". On constate que X est un sous-groupe de G. Par l'absurde, supposons $X \neq G$. On a donc X fini, si bien que, par le théorème d'isomorphisme (on pourrait aussi justifier ça à la main avec le lemme des tiroirs), $Ker(f)$ serait infini. L'hypothèse faite sur G impose donc que l'on a $G = Ker(f)$ donc tout les éléments de G sont d'ordre 1 ou p. Or, il n'y a qu'un nombre fini d'éléments d'ordre p, absurde puisque G est infini.

   On peut donc construire une suite $(a_n) \in G^{\mathbb{N}}$ telle que pour tout $n \in \mathbb{N}$, a_n est d'ordre p^n et $a_{n+1}^p = a_n$. Comme $< a_n >_{n\in\mathbb{N}}$ est infini, on a $G =< a_n >_{n\in\mathbb{N}}$ et on peut conclure comme en q.1.

1.11 Groupe diédral

Soit $n \in \mathbb{N}^*$, notons $(A_k)_{0\leqslant k\leqslant n-1}$ les points du plan euclidien E d'affixe $(e^{2i\pi k/n})_{0\leqslant k\leqslant n-1}$ et notons $\mathcal{P}_n = \{A_0, \cdots, A_{n-1}\}$ le polygone régulier à n sommets. Posons

$$D_{2n} = \{f \in O(E) : f(\mathcal{P}_n) = \mathcal{P}_n\}$$

le groupe des isométries de $\mathcal{P}_n$ (il arrive que certaines personnes choisissent de noter D_n au lieu de D_{2n}).

1. Montrer que D_{2n} est un sous-groupe de $O(E)$. On l'appelle groupe diédral d'ordre $2n$.

   Notons r la rotation d'angle $2\pi/n$ et s la symétrie orthogonale par rapport à l'axe des abscisses.

2. Soit $f \in D_{2n}$.

   (a) Justifier qu'il existe des entiers k, l tels que $(f(A_0), f(A_1)) = (A_k, A_l)$ et $l = k+1 \mod n$ ou $l = k-1 \mod n$.

   On pourra vérifier que la distance entre A_k et A_l est $2|\sin((k-l)\pi/n)$

   (b) En déduire qu'il existe $k \in [\![0, n[\![$ tel que $f = r^k$ ou $f = r^k \circ s$.

   (c) Conclure que l'on a
   $$D_{2n} = \left\{s^a r^b : 0 \leqslant a \leqslant 1, 0 \leqslant b < n\right\}.$$
   Quel est l'ordre de D_{2n} ?

   (d) Montrer que D_{2n} est le groupe engendré par s, s' ou s' désigne la symétrie orthogonale par rapport à la droite vectorielle dirigée par le vecteur $(\cos(\pi/n), \sin(\pi/n))$.

1.12 Groupe diédral infini (*)

Soit θ un réel tel que θ/π ne soit pas rationnel. Dans le plan euclidien E, notons s la symétrie orthogonale par rapport à l'axe des abscisses et s' la symétrie orthogonale par rapport à la droite vectorielle dirigée par le vecteur $(\cos(\theta), \sin(\theta))$. On considère D_∞ le groupe (diédral infini) engendré par s, s'.

1. En considérant $r = s' \circ s$, montrer que D_∞ est infini et non commutatif.
2. Montrer que les sous-groupes stricts de D_∞ sont les groupes finis $\{1, s\}$ et $\{1, s'\}$.
3. Montrer que D_∞ est également engendré par $\{r, s\}$.

1.13 Automorphismes involutifs n'ayant qu'un seul point fixe (Oral ENS Cachan 2015)(**)

1. Soit G un groupe fini. On suppose qu'il existe un automorphisme $\varphi : G \to G$ involutif (i.e. $\varphi \circ \varphi = \mathrm{Id}_G$) admettant un unique point fixe.

   (a) Montrer que φ est l'application $g \mapsto g^{-1}$.

   On pourra écrire les éléments de G sous la forme $\varphi(x)x^{-1}$.

(b) En déduire que G est abélien et de cardinal impair.

2. Exhiber un groupe non commutatif G possédant un automorphisme involutif n'ayant qu'un seul point fixe.

1.14 Autour de l'ordre

Soit G un groupe abélien.

1. Soient $x, y \in G$ d'ordre n, m. On suppose que l'on a $n \wedge m = 1$. Montrer que xy est d'ordre nm. Ce résultat tient-il toujours sans l'hypothèse $n \wedge m = 1$.
2. Soit $g \in G$ d'ordre n. Si d est un entier, montrer que g^d est d'ordre $n/\operatorname{pgcd}(n, d)$.
3. Construire un élément $g \in G$ d'ordre

$$d = \operatorname{ppcm}(o(x) : x \in G).$$

et justifier que d est le plus grand entier n tel qu'il existe un élément de G d'ordre n.

On pourra décomposer d en produit de puissances de nombres de premiers.

1.15 Ordre dans le groupe quotient (Josette Calais, Elements de théorie des groupes) (*)

Soit G un groupe. On suppose qu'il existe un sous-groupe H normal dans G et d'ordre fini m. Si $pgcd(n, m) = 1$, montrer que l'on a l'implication :

$$o(\bar{x}) = n \implies \exists y \in \bar{x} : o(y) = n.$$

On pourra chercher à montrer que x^n admet une racine n^{eme} dans H.

1.16 Groupes non isomorphes (*)

Soit $(K, +, \times)$ un corps. Montrer que les groupes $(K, +)$ et $(K^*, \times)$ ne sont pas isomorphes.

1.17 Cyclicité

Soit $\mathbb{K}$ un corps. Montrer que tout sous-groupe fini de $(\mathbb{K}^*, \times)$ est cyclique.

Si n est l'ordre d'un tel sous-groupe, on pourra s'intéresser au polynôme $X^n - 1$ et s'en inspirer.

1.18 Autour des groupes cycliques

Soit $n \in \mathbb{N}^*$. Soit $d \mid n$.

1. Montrer que le groupe engendré par n/d est le seul sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.
2. Combien d'éléments d'ordre 2 y a t-il dans $\mathbb{Z}/n\mathbb{Z}$? Ce résultat peut-il s'étendre à un autre ordre que 2 ?

1.19 Cyclicité et unités

Le but de cet exercice est de montrer que le groupe $\mathbb{Z}/n\mathbb{Z}^\times$ est cyclique si et seulement si n est 2 ou 4 ou de la forme p^a ou $2p^a$ pour un certain entier a et un nombre premier impair p.

1. Montrer que si $\mathbb{Z}/n\mathbb{Z}^\times$ est cyclique alors n une puissance d'un nombre premier (pas nécessaire impair) ou le double d'une telle puissance.

   On pourra utiliser le théorème des restes chinois et étudier les éléments d'ordre 2.

2. On suppose ici que l'on a $n = p^a$ avec p impair.

   (a) Montrer que pour tout $k \geqslant 0$, il existe $\lambda_k \in \mathbb{Z}$ tel que

   $$(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$$

   et $p \nmid \lambda_k$.

   (b) Montrer que $1 + p \in \mathbb{Z}/n\mathbb{Z}^\times$ est d'ordre p^{a-1}.

   (c) En considérant le morphisme naturel $\mathbb{Z}/p^a\mathbb{Z}^\times \to \mathbb{Z}/p\mathbb{Z}^\times$, justifier qu'il existe un élément d'ordre $p-1$ dans $\mathbb{Z}/n\mathbb{Z}^\times$ et conclure que ce dernier groupe est cyclique.

3. On suppose ici que l'on a $n = 2^a$ avec $a \geqslant 2$.

   (a) Montrer que pour tout $k \geqslant 0$, il existe $\lambda_k \in \mathbb{Z}$ impair tel que

   $$5^{2^k} = 1 + \lambda_k 2^{2^{k+2}}.$$

   (b) Montrer que $5 \in \mathbb{Z}/n\mathbb{Z}^\times$ est d'ordre 2^{a-2}.

   (c) Montrer que le morphisme naturel $\mathbb{Z}/2^a\mathbb{Z}^\times \to \mathbb{Z}/4\mathbb{Z}^\times = \mathbb{Z}/2\mathbb{Z}$ est surjectif et que $5 \in \mathbb{Z}/2^a\mathbb{Z}^\times$ engendre son noyau. En déduire que l'on a

   $$\mathbb{Z}/n\mathbb{Z}^\times \simeq \mathbb{Z}/2^{a-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

   On montrera cet isomorphisme proprement. En particulier, on n'invoquera pas d'argument sorti du chapeau comme "j'ai G/H isomorphe à K donc j'ai G isomorphe à $H \times K$.

4. Conclure.

2 Polynômes

2.1 Divisibilité dans $\mathbb{Z}$

Soient $P, Q \in \mathbb{Z}[X]$ tels que $\{n : P(n) \mid Q(n)\}$ soit infini. Montrer que P divise Q dans $\mathbb{Q}[X]$.

2.2 Irréductibilité (1) (Tosel)

Soient $n \in \mathbb{N}^*$ et $a_1, ..., a_n$ des entiers 2 à 2 distincts. Montrer l'irréductibilité de $P = \prod_{k=1}^{n} (X - a_i) - 1$ dans $\mathbb{Q}[X]$.

2.3 Irréductibilité (2) (Tosel)

1- Montrer qu'un polynôme de $\mathbb{Z}[X]$ prenant 4 fois la valeur 1 sur $\mathbb{Z}$ ne peut pas prendre la valeur -1 sur $\mathbb{Z}$

2- En déduire que pour tout $n \geq 12$ et $P \in \mathbb{Z}[X]$ de degré n prenant les valeurs ± 1 en au moins $\lfloor \frac{n}{2} \rfloor + 1$ entiers est irréductible.

2.4 Groupe de torsion (Tosel)

1- Montrer que $\varphi(n) \xrightarrow[n\to\infty]{} \infty$ où φ désigne l'indicatrice d'Euler.

2-Soit $\mathbb{K}$ une extension finie de $\mathbb{Q}$. Déduire de la question précédente que $Tor(\mathbb{K}^*)$ est fini.

2.5 Généralisation d'un résultat d'irréductibilité (moi)

Il est bien connu que si l'on se donne un corps $\mathbb{K}$ de caractéristique p et $x \in \mathbb{K}$ tel que x n'ait pas de racine p^{eme} dans $\mathbb{K}$ alors $X^p - x$ est irréductible sur $\mathbb{K}$.

Soit $\mathbb{L}/\mathbb{K}$ une extension, les deux corps étant de caractéristique quelconque et soit p premier. On se donne $Q \in \mathbb{L}[X]$ tel que Q soit unitaire, irréductible sur $\mathbb{L}[X]$, $Q \notin \mathbb{K}[X]$ et $Q^p \in \mathbb{K}[X]$. Montrer que Q^p est irréductible sur $\mathbb{K}[X]$. Expliquer en quoi cela est une généralisation du résultat mentionné plus haut.

2.6 Dénombrement des irréductibles dans $\mathbb{F}_q[X]$

Soient $p \in \mathbb{P}$, $n > 0$, $q = p^n$, $A(m,q)$ l'ensemble des irréductibles de degré m de $\mathbb{F}_q[X]$ et $I(m,q)$ sont cardinal.

1- Montrer que l'on a $X^{q^m} - X = \prod_{d|m} \prod_{P \in A(d,q)} P(X)$.

2- Montrer que l'on a $I(m,q) = \frac{1}{m} \sum_{d|m} \mu(\frac{m}{d}) q^d$.

3- En déduire $I(m,q) \underset{m\to\infty}{\sim} \frac{q^m}{m}$.

Remarque: En particulier, pour m assez grand, on sait qu'il existe un irréductible de degré m dans $\mathbb{F}_q[X]$. En fait, on peut montrer que pour tout m, $I(m,q) > 0$ en utilisant que les extensions de degré m de $\mathbb{F}_q$ sont données par quotient de $\mathbb{F}_q[X]$ par un irréductibles de degré m.

3 Nombres algébriques

3.1 Nombres de Salem (Tosel)

Un nombre de Salem est un entier algébrique x (irrationnel) vérifiant $x \in]1; +\infty[$ et tel que toutes les racines de π_x autres que x ($\pi_x \in \mathbb{Z}[X]$ désigne le polynôme minimal de x sur $\mathbb{Q}$) soient de module plus petit que 1 mais qu'il en existe au moins une de module exactement 1.

1- Pour un tel x, montrer que π_x est un polynôme réciproque et que toutes les racines différentes de x et $\dfrac{1}{x}$ sont de module 1.

2- Montrer que le degré de x est un entier pair plus grand que 4.

3.2 Nombres de Pisot

Un nombre de Pisot-Vijayaraghavan est un entier algébrique réel strictement supérieur à 1, dont tous les éléments conjugués ont un module strictement inférieur à 1.

1- Montrer que $1+\sqrt{3}$ et le nombre d'or sont des nombres de Pisot.

2- Soit $n \geqslant 2$. Montrer que $X^n - \sum_{i=0}^{n-1} X^k$ admet une unique racine réelle positive et que ce réel est un nombre de Pisot.

3- Montrer que tout corps de nombre réel $\mathbb{K}$ est engendré par un nombre de Pisot.

Indication: On se servira du théorème de Minkowski avec la matrice $M = (\sigma(\alpha^j))_{\sigma,j}$ où σ parcourt l'ensemble des $\mathbb{K} \to \overline{\mathbb{Q}}$ et α est un entier algébrique engendrant $\mathbb{K}$.

4 Extensions de corps

4.1 Nombre de corps de rupture

Soit $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$ un polynôme séparable irréductible. Soit Ω une clotûre algébrique de $\mathbb{K}$. Montrer que le nombre N de corps de rupture de P inclus dans Ω divise le degré de P.

4.2 Caractérisation des extensions finies séparables

Soit $\mathbb{L}/\mathbb{K}$ une extension algébrique séparable telle qu'il existe M vérifiant

$[\mathbb{K}[x] : \mathbb{K}] < M$ pour tout $x \in \mathbb{L}$. Montrer que $\mathbb{L}$ est une extension finie.

4.3 Parfaitude et extensions

Soit $\mathbb{L}/\mathbb{K}$ une extension finie de corps. Montrer que $\mathbb{L}$ est un corps parfait si et seulement si $\mathbb{K}$ est parfait.

4.4 Irréductibilité et extension

Soit $\mathbb{L}/\mathbb{K}$ une extension de degré impair. Montrer que si P est irréductible sur $\mathbb{K}[X]$ alors P est également irréductible sur $\mathbb{L}[X]$.

4.5 Théorème de Springer*

Soit $\mathbb{K}$ un corps.

1. Montrer que les deux conditions suivantes sont équivalentes

(a) L'ensemble

$$\left\{(x_1,\dots,x_r)\in\mathbb{K}^r : \sum_{i=1}^{r} x_i^2 = 0\right\}$$

est réduit à 0 pour tout $r\in\mathbb{N}^*$

(b) -1 ne s'écrit pas comme somme de carrés dans $\mathbb{K}$.

2. On suppose que $\mathbb{K}$ vérifie la condition précédente. Soit $\mathbb{L}/\mathbb{K}$ une extension finie de degré impair. Montrer que $\mathbb{L}$ vérifie également cette propriété.

Proof. Quitte à faire des pas petit à petit, on peut supposer $\mathbb{L} = \mathbb{K}(x)$ (sinon on démontre la propriété avec $\mathbb{K}(x_1)$ puis on pourra faire de même avec l'extension $\mathbb{K}(x_1,x_2)/\mathbb{K}(x_1)$ etc). Par l'absurde, supposons que $\mathbb{L}$ ne satisfait pas la condition de la question 1 et que $\mathbb{L}$ est de degré minimal pour cette propriété. Soient $P_1,\dots,P_r\in\mathbb{K}[X]\setminus\{0\}$ tels que

$$0=\sum_{i=1}^{r} P_i(x)^2.$$

Il existe alors un polynôme $Q\in\mathbb{K}[X]$ tel que

$$\sum_{i=1}^{r} P_i^2 = \pi_x Q.$$

Notons n le degré de x et remarquons que le polynôme de gauche est de degré inférieur ou égal à $2(n-1)$. De plus, le polynôme de gauche est de degré pair grâce au fait que $\mathbb{K}$ satisfait l'hypothèse de la question 1. Ainsi, Q est un polynôme de degré impair et de degré strictement inférieur à n. Par conséquent, il existe y (dans la clôture algébrique de $\mathbb{K}$) tel que $\pi_y \mid Q$, le degré de y est impair, strictement inférieur à n et la valuation de π_y dans Q est impaire. Ainsi, $\mathbb{K}(y)$ vérifie l'énoncé de la question 1, de sorte que l'on obtient $\pi_y \mid P_i$ pour tout i puis en jouant sur la valuation de π_y, on peut conclure à une absurdité (imaginons que la valuation est 1, en écrivant $P_i=\pi_y R_i$, on obtient clairement une absurdité en injectant cela dans l'équation définissant Q et si la valuation n'est pas 1, on s'y ramène petit à petit en divisant par π_y^2 dans l'équation définissant Q). □

4.6 Extensions infinies

Soit $\mathbb{L}/\mathbb{K}$ une extension algébrique infinie de caractéristique nulle. Montrer que $\mathbb{L}$ contient des éléments de degré arbitrairement grand.

Que se passe-t-il si l'extension est de caractéristique finie ?