Université de Toulon
U.F.R. de Sciences
Mathématiques

Année 2017/2018

Licence de Mathématiques - 3ème année

Algèbre

Unité d'enseignement M-54

Travaux Dirigés

Yves Aubry

.

Université de Toulon
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Année 2017/2018

Première partie

.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *Evariste Galois (1811-1832)*
Licence 3-ième année

Algèbre T.D. - 1

Exercice. Construction de $\mathbb{Z}$ (ou plus généralement, symétrisation d'un semi-groupe)

Quiz : Exemples (ou non) de groupes

Les ensembles suivants munis de la loi indiquée sont-ils des groupes ?

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Z}, \times)$
3. $(\mathbb{Z} - \{0\}, \times)$, $(\mathbb{Z}^*, \times)$.
4. L'ensemble des entiers relatifs pairs muni de l'addition.
5. L'ensemble des entiers relatif impairs muni de l'addition.
6. $(\mathbb{Q}, +)$
7. $(\mathbb{Q}, \times)$
8. $(\mathbb{Q}^*, \times)$
9. $(\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}, +)$
10. $(\mathbb{Q}(i\sqrt{5})^* = \{a + ib\sqrt{5}, a, b \in \mathbb{Q}, (a, b) \neq (0, 0)\}, \times)$
11. $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \times)$
12. L'ensemble des racines n-ième de l'unité $\mu_n = \{e^{\frac{2ik\pi}{n}}, k = 0, \ldots, n-1\}$ muni de la multiplication.
13. L'ensemble $\mathfrak{S}_X$ des permutations d'un ensemble X (i.e. des bijections de X) muni de la loi de composition des applications.
14. $(\mathcal{P}(E), \cap)$ où $\mathcal{P}(E)$ est l'ensemble des parties d'un ensemble E.
15. $(\mathcal{P}(E), \cup)$
16. $(\mathcal{P}(E), \Delta)$ où Δ est la différence symétrique $(A \Delta B = A \cup B - A \cap B = (A - B) \cup (B - A))$
17. $(\mathcal{M}_n(\mathbb{R}), +)$
18. $(\mathcal{M}_n(\mathbb{R}), \times)$
19. $(\mathrm{GL}_n(\mathbb{R}), \times)$
20. L'ensemble $\{0, 1\}$ muni de l'addition avec $1 + 1 = 0$.

Exercice. Montrer que tout semi-groupe fini est un groupe.

(Rappelons qu'un semi-groupe est un ensemble muni d'une loi de composition interne associative telle que tout élément soit régulier (à droite et à gauche)).

Remarquons que cela montre que tout anneau fini intègre est un corps (rappellons qu'il suffit pour cela de montrer que tout élément non nul (i.e. différent de l'élément neutre de la première loi) de l'anneau est inversible (i.e. admet un symétrique pour la seconde loi).

De manière analogue, on montre que toute partie non vide, stable et finie d'un groupe en est un sous-groupe.

Exercice. Soient $(G, *)$ et $(H, \top)$ deux groupes ; soient f et g deux morphismes de $(G, *)$ dans $(H, \top)$. Notons

$$K = \{x \in G \mid f(x) = g(x)\}.$$

Montrer que $(K, *)$ est un sous-groupe de $(G, *)$.

Exercice. Groupes d'exposant 2.
Montrer qu'un groupe dans lequel tout élément non neutre est d'ordre 2 est nécessairement abélien.
Donner un exemple de tel groupe.

Exercice. Montrer que tout groupe fini d'ordre pair admet au moins un élément d'ordre 2.

Exercice. Groupes d'ordre p premier.
Soit G un groupe d'ordre p premier. Montrer que G est alors nécessairement cyclique et peut être engendré par l'un quelconque de ses éléments autre que l'élément neutre. En déduire que G est abélien.

Exercice. Groupes d'ordre 4.
1) Montrer que la table de Pythagore d'un groupe G est un carré latin, i.e. que chaque élément de G figure une et une seule fois dans chaque rangée (ligne ou colonne). La réciproque est-elle vraie ?

2) Soit $G = \{e, a, b, c\}$ un groupe d'ordre 4, d'élément neutre e. Construire les tables possibles de G.

Exercice. Intersection et réunion de sous-groupes.
Soit G un groupe et H et K deux sous-groupes de G.

1) Montrer que $H \cap K$ est un sous-groupe de G.

2) Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.

Exercice. Si H et K sont deux sous-groupes d'un groupe G, on définit :

$$HK = \{hk, h \in H, k \in K\}.$$

L'ensemble HK est-il nécessairement un sous-groupe de G ?
(On pourra considérer le cas particulier où $G = \mathfrak{S}_3$, $H =< \tau_1 >$ et $K =< \tau_2 >$ où $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \quad 3)$ et $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \quad 3)$).

Exercice. Montrer que si H et K sont deux sous-groupes d'un groupe fini G alors :

$$\sharp HK = \frac{\mid H \mid \times \mid K \mid}{\mid H \cap K \mid}$$

Un exemple : groupe non abélien.
Soit $E = \{1, 2, 3\}$ et $\mathfrak{S}_3 = S(E)$ le groupe symétrique de E. On a :

$$\mathfrak{S}_3 = \{e, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}$$

avec $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \quad 3)$, $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \quad 3)$, $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \quad 2)$, $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3)$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \quad 3 \quad 2)$.

Ecrire la table de $(\mathfrak{S}_3, \circ)$ et déterminer tous ses sous-groupes.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *Joseph Louis Lagrange (1736-1813)*
Licence 3-ième année

Algèbre T.D. - 2

Exercice. Centre d'un groupe
Soit $(G, .)$ un groupe. On appelle centre de G, l'ensemble $Z(G) = \{x \in G \mid x.y = y.x \ \forall y \in G\}$.

1) Montrer que $Z(G)$ est un sous-groupe distingué de G (il est évidemment égal à G si et seulement si G est commutatif).

2) Quel est le centre de $\mathfrak{S}_3$? De $\mathrm{GL}_2(\mathbb{R})$? Du groupe quaternonien ?

3) Montrer que si $G/Z(G)$ est cyclique alors G est commutatif.

4) En utilisant le fait que le centre d'un p-groupe est non trivial (Théorème de Burnside), montrer que tout groupe d'ordre p^2, avec p premier, est commutatif.

Exercice. Centralisateur d'un élément. Soit x un élément d'un groupe G ; on appelle centralisateur de x le sous-groupe de G suivant : $C_x = \{y \in G \mid x.y = y.x\}$.
Montrer que

$$Z(G) = \bigcap_{x \in G} C_x \quad \text{et} \quad x \in Z(G) \Longleftrightarrow C_x = G$$

Exercice. Groupe des automorphismes intérieurs.
Soit G un groupe et $\mathrm{Aut}(G)$ le groupe des automorphismes de G. Soit $g \in G$ et i_g l'application

$$\begin{array}{rccc} i_g : & G & \longrightarrow & G \\ & x & \longmapsto & gxg^{-1} \end{array}$$

Montrer que i_g est un automorphime de G appelé automorphisme intérieur de G associé à l'élément g.
Soit $\mathrm{Int}(G) = \{i_g \mid g \in G\}$ l'ensemble des automorphismes intérieurs de G. Montrer que $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$ et que $G/Z(G) \simeq \mathrm{Int}(G)$ où $Z(G)$ désigne le centre de G.

Exercice. Ordre d'un produit : exemples
1) Montrer que les éléments $a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $b = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ dans $\mathrm{GL}(2, \mathbb{R})$ sont d'ordre fini mais que ab est d'ordre infini.

2) Montrer que les éléments $a = (0, 1)$ et $b = (1, -1)$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ sont d'ordre infini mais que $a + b$ est d'ordre fini.

Exercice. Ordre d'un produit
Soit G un groupe multiplicatif d'élément neutre e et soient a et b deux éléments d'ordre fini de G.
1) Montrer que

$$a^r = e \iff \mathrm{ord}(a) \mid r$$

2) Montrer que l'ordre de ab est égal à l'ordre de ba.

3) Montrer que si a et b commutent entre eux alors l'ordre du produit est fini et divise le PPCM des ordres de a et de b.

4) Montrer que si a et b commutent entre eux et si leurs ordres sont premiers entre eux alors :

$$\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$$

Exercice. Ordre dans un produit.
Soient H et K deux groupes finis et soient $h \in H$ et $k \in K$. Montrer que l'ordre de (h, k) dans $H \times K$ est le PPCM de l'ordre de h dans H et de l'ordre de k dans K.

Exercice. Ordre dans un groupe cyclique.
Soit $G = \langle x \rangle$ un groupe cyclique d'ordre n engendré par x. Montrer que, pour tout $k \in \mathbb{N}$:

$$\mathrm{ord}(x^k) = \frac{n}{(n, k)}$$

En corollaire, on a donc que $\mathrm{ord}(x^d) = \frac{n}{d}$ *si* d *divise* n *et que* x^k *engendre* G *si et seulement si* $(n, k) = 1$.

Exercice. Ordre dans un quotient.
Soit H un sous-groupe distingué d'un groupe G et soit $g \in G$. Montrer que l'ordre de gH dans G/H divise l'ordre de g dans G.

Exercice. Ordre par un isomorphisme.
Montrer que l'ordre d'un élément est préservé par isomorphisme.
En particulier, l'image d'un générateur par un isomorphisme est un générateur.

Un exemple : Groupe infini dont tous les éléments sont d'ordre fini.
Il est clair que si G est un groupe fini, tout élément de G est d'ordre fini. Mais qu'en est-il de la réciproque ? On pourra considérer le groupe infini $\mathbb{Q}/\mathbb{Z}$ et montrer que tous ses éléments sont d'ordre fini.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *William Rowan Hamilton (1805-1865)*
Licence 3-ième année

Algèbre T.D. - 3

Exercice : Groupe des Quaternions.
Il est clair que tout sous-groupe d'un groupe abélien est distingué. Qu'en est-il de la réciproque ? Voici un exemple de groupe non abélien dont tous les sous-groupes sont distingués.

Soient $\mathbb{H}$ le corps des quaternions (surcorps non commutatif de $\mathbb{C}$), et $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$. On rappelle que l'on a : $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ et $ki = -ik = j$.

Montrer que $\mathbb{H}_8$ est un groupe non abélien, appelé groupe des quaternions ou groupe quaternonien. Déterminer les sous-groupes de $\mathbb{H}_8$ et montrer qu'ils sont tous distingués.

Exercice. Considérons les matrices $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ de $\mathrm{GL}(2, \mathbb{C})$.
Montrer que le groupe engendré par A et B est un groupe d'ordre 8 qui est isomorphe au groupe des quaternions.

Exercice : groupe donné par générateurs et relations.
Soit G le groupe engendré par les éléments a et b satisfaisant les relations :

$$a^4 = e, \quad a^2 = b^2, \quad aba = b$$

Montrer que G est isomorphe au groupe des Quaternions.

Exercice : Groupe Diédral.
Rappelons que le groupe diédral D_n est le groupe des isométries du plan euclidien conservant un polygone régulier à n côtés.
Il contient les n rotations $r(O, 2k\pi/n)$ de centre O, le centre du polygone, pour $k = 0, \ldots, n-1$, et les n réflexions par rapport aux droites passant par O et les sommets ou les milieux des côtés du polygone.

1) Montrer que le groupe G engendré par les matrices $A = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ dans $\mathrm{GL}(2, \mathbb{C})$ est isomorphe au groupe diédral D_n.

2) Montrer que le groupe engendré par les éléments a et b satisfaisant les relations :

$$a^n = e, \quad b^2 = e, \quad abab = e$$

est isomorphe au groupe diédral D_n.

Exercice. Nombres de Fermat

1) Montrer que si $2^p + 1$ est premier alors il existe un entier n tel que $p = 2^n$.

2) Soit $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Montrer que si un nombre premier p divise F_n alors $p \equiv 1 \bmod 2^{n+1}$.

Exercice. Nombres de Mersenne

Soit $M_p = 2^p - 1$ le p-ième nombre de Mersenne.

1) Montrer que si M_p est premier alors p est premier.

2) On suppose que p est premier. Montrer que si q est un nombre premier qui divise M_p alors $q \equiv 1 \bmod 2p$.

Exercice. Soient G un groupe fini et ρ un morphisme de G dans $\mathrm{GL}_n(\mathbb{C})$. Montrer que pour tout g dans G, $\rho(g)$ est diagonalisable.

Exercice. Montrer que l'ordre d'un élément de $\mathfrak{S}_n$ est au plus $e^{\frac{n}{e}}$ où e est la base du logarithme népérien.

Exercice. Soient p un nombre premier et k un entier. En considérant une racine primitive modulo p, montrer que la somme

$$S_k = \sum_{i=1}^{p-1} i^k$$

est divisible par p lorsque $p - 1$ ne divise pas k ; sinon, que vaut-elle modulo p ?

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *Félix Klein (1849-1925)*
Licence 3-ième année

Algèbre T.D. - 4

Exercice. Morphismes injectifs.
Montrer qu'un morphisme de groupes est injectif si et seulement si son noyau est réduit à l'élément neutre.

Exercice. Soit $f : G \longrightarrow G'$ un morphisme de groupes. Montrer que si $H' \triangleleft G'$ alors $f^{-1}(H') \triangleleft G$. En déduire que $\mathrm{Ker}\, f \triangleleft G$.

Exercice. 1) Soit G un groupe. Montrer que l'application $x \longmapsto x^{-1}$ de G dans G est un automorphisme de G si et seulement si G est abélien.

Dans tout ce qui suit, on suppose que G est un groupe fini non abélien.
Soit $\tau \in \mathrm{Aut}(G)$ vérifiant $\tau \circ \tau = \mathrm{id}$. On veut démontrer qu'alors τ fixe au moins un élément différent de l'élément neutre e, i.e. qu'il existe $x \in G$ tel que $x \neq e$ et $\tau(x) = x$.

Supposons au contraire que τ ne fixe que e, i.e. que $\tau(x) = x$ entraîne $x = e$. Alors :

2) Montrer que l'application $\varphi : x \longmapsto x^{-1}\tau(x)$ est injective.

3) Montrer que pour tout $x \in G$, il existe $y \in G$ tel que $x = y^{-1}\tau(y)$.

4) En déduire que τ fixe au moins un élément différent de l'élément neutre e.

Exercice. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.
Soit $a \in \mathbb{Z}$; montrer que les propriétés suivantes sont équivalentes :

1) $\bar{a}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$
2) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, i.e. $\bar{a}$ est inversible dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$
3) $(a, n) = 1$.

Exercice. Quel est le nombre d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$?

Exercice. Déterminer tous les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$.

Exercice. Montrer que pour tout entier naturel n, on a :

$$n = \sum_{d|n} \varphi(d)$$

où φ est la fonction indicatrice d'Euler.

En déduire que le nombre d'éléments d'ordre divisant k dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $\mathrm{PGCD}(n, k)$.

Exercice. Quels sont les éléments d'ordre 5 de $\mathbb{Z}/20\mathbb{Z} \times \mathfrak{S}_3$?

Exercice. Soient m_1 et m_2 deux entiers naturels premiers entre eux et soient a_1 et a_2 deux entiers. Trouver un entier a tel que

$$\begin{cases} a & \equiv & a_1 & \mod & m_1 \\ a & \equiv & a_2 & \mod & m_2 \end{cases}$$

Quelles sont toutes les solutions entières de ce système ?

Résoudre de même le système de n congruences $a \equiv a_i \bmod m_i$ pour $i = 1, \ldots, n$ où les m_i sont des entiers deux à deux premiers entre eux.

Exercice. Le problème du cuisinier chinois.

Une bande de dix-sept pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait alors trois pièces. Mais les pirates se querellent et six d'entre-eux sont tués. Le cuisinier recevrait alors quatre pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés et le partage laisserait cinq pièces d'or à ce dernier.
Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Exercice. Trouver tous les éléments d'ordre 6 de $(\mathbb{Z}/65\mathbb{Z})^*$.

Exercice. Combien y-a-t-il d'éléments d'ordre 2 dans $(\mathbb{Z}/57\mathbb{Z})^*$?

Exercice. Trouver un entier $n \in \mathbb{N}$ différent de 57 tel que $(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/57\mathbb{Z})^*$.

Exercice. Trouver un élément d'ordre 6 du groupe $(\mathbb{Z}/175\mathbb{Z})^*$.

Exercice. Théorèmes d'Euler, Fermat et Wilson
1) Théorème d'Euler.
Montrer que si $(a, m) = 1$ alors $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

2) Petit théorème de Fermat.
Montrer que si p est premier et si p ne divise pas a alors $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

3) Théorème de Wilson.
Montrer que si p est premier alors $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.

4) Déterminer le reste de la division euclidienne de $(103!)^{109}$ par 107.

Exercice. Montrer que tout groupe d'ordre p^2, avec p premier, est soit isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, soit isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice. Déterminer les classes à gauches et les classes à droite modulo les deux sous-groupes $H = \{e, \tau_1\}$ et $\mathfrak{A}_3$ de $\mathfrak{S}_3$.

Déterminer tous les sous-groupes distingués de $\mathfrak{S}_3$.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *William Burnside (1852-1927)*
Licence 3-ième année

Algèbre T.D. - 5

Exercice.
1) Soit E un ensemble fini de cardinal n, et soit e un élément de E. On considère l'ensemble B des bijections de E sur lui-même qui fixent e. Quel est le cardinal de B ?
2) On considère le groupe $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Montrer que les applications ϕ et ψ définies sur $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par $\phi\big((a,b)\big) = (b, a+b)$ et $\psi\big((a,b)\big) = (b,a)$ sont des éléments de $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Quels sont leurs ordres ?
3) Déterminer l'ordre de $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.
4) Montrer que $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ n'est pas abélien.

Exercice. Quel est le cardinal de $\mathrm{Aut}(\mathrm{Aut}(\mathbb{Z}/109\mathbb{Z}))$? Combien contient-il d'éléments d'ordre 6 ?

Exercice. Pour tout entier $n \geq 1$, on note μ_n le sous-groupe de $\mathbb{C}^*$ engendré par $e^{\frac{2i\pi}{n}}$. Pour tout groupe H, on note $\mathrm{Aut}(H)$ son groupe d'automorphismes. On pourra admettre que les nombres 593 et 761 sont premiers.
1) Le groupe μ_{593} est-il fini ?
2) Combien a-t-il de sous-groupes ?
3) Calculer le cardinal du groupe $\mathrm{Aut}(\mathrm{Aut}(\mu_{593}))$.
4) Les groupes $\mathrm{Aut}(\mathrm{Aut}(\mu_{593}))$ et $\mathrm{Aut}(\mathrm{Aut}(\mu_{761}))$ sont-ils isomorphes ?

Exercice. Groupe dérivé.
Soit G un groupe et $D(G)$ son groupe dérivé.
1) Montrer que le symétrique d'un commutateur est un commutateur.
2) Montrer que $D(G) \triangleleft G$.
3) Montrer que G est abélien si et seulement si $D(G) = \{e\}$.
4) Si $H \triangleleft G$, montrer alors que :

$$G/H \ \text{ commutatif } \iff D(G) \subset H$$

5) Montrer que $D(\mathfrak{S}_3) = \mathfrak{A}_3$ et que $D(\mathfrak{A}_4) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice. Soit $\Gamma = \mathrm{SL}(2,\mathbb{Z})$ le groupe spécial linéaire défini par :

$$\Gamma = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}, ad-bc=1\}.$$

Soit p un nombre premier et soit $\Gamma(p)$ la partie de Γ définie par :

$$\Gamma(p) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \bmod p\}.$$

1) Montrer que $\Gamma(p)$ est un sous-groupe de Γ. Est-il distingué dans Γ ?

2) Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de Γ qui n'appartient pas à $\Gamma(p)$. Montrer qu'il existe un élément γ' de Γ de la forme $\begin{pmatrix} a' & b' \\ 1 & d' \end{pmatrix}$ tel que $\gamma\Gamma(p) = \gamma'\Gamma(p)$.

3) Trouver un système de représentants de l'ensemble des classes à droite $\Gamma/\Gamma(p)$. Déterminer $[\Gamma : \Gamma(p)]$.

Exercice. Considérons le groupe symétrique $\mathfrak{S}_4$ et deux de ses sous-groupes H et K suivants :

$$H = \{e, (12)(34)\} \quad \text{et} \quad K = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Montrer $H \lhd K$ et $K \lhd \mathfrak{S}_4$ mais que H n'est pas distingué dans $\mathfrak{S}_4$.

Un exemple : Sous-groupe distingué non caractéristique.
Rappelons qu'un sous-groupe d'un groupe G est distingué dans G s'il est invariant par automorphisme intérieur ; il est dit caractéristique s'il est invariant par tout automorphisme.

Montrer que l'application

$$\begin{array}{rccc} f: & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ & (x,y) & \longmapsto & (y,x) \end{array}$$

est un automorphisme de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Montrer que le sous-groupe $H = \mathbb{Z}/2\mathbb{Z} \times \{0\}$ de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est distingué mais pas caractéristique.

Un exemple : Groupe isomorphe à son groupe d'automorphismes.
En considérant l'application

$$\begin{array}{rccc} f: & \mathfrak{S}_3 & \longrightarrow & \mathrm{Aut}(\mathfrak{S}_3) \\ & s & \longmapsto & (f_s : r \mapsto s \circ r \circ s^{-1}) \end{array}$$

montrer que le groupe symétrique $\mathfrak{S}_3$ est isomorphe à son groupe d'automorphismes $\mathrm{Aut}(\mathfrak{S}_3)$.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *Augustin-Louis Cauchy (1789-1857)*
Licence 3-ième année

Algèbre T.D. - 6

Exercice : Second théorème d'isomorphisme.
Soient G un groupe, $K \lhd G$ et H un sous-groupe de G.
Montrer que :
- $H \cap K \lhd H$
- HK est un sous-groupe de G

et

$$H/H \cap K \simeq HK/K$$

Exercice. Soit $\tau = (12) \in \mathfrak{S}_n$ et H le sous-groupe de $\mathfrak{S}_n$ engendré par τ. Montrer que $H\mathfrak{A}_n/\mathfrak{A}_n$ est cyclique d'ordre 2. (*Utiliser le second théorème d'isomorphisme.*)

Exercice : Troisième théorème d'isomorphisme.
Soient H et K deux sous-groupes distingués d'un groupe G. On suppose que $K \subset H$. Montrer alors que $H/K \lhd G/K$ et que

$$(G/K)/(H/K) \simeq G/H$$

Exercice : Produit semi-direct.
1) Soit G un groupe dont A et B sont des sous-groupes. On rappelle que G est produit semi-direct de B par A si les trois conditions suivantes sont satisfaites :
a) $G = AB$
b) $A \cap B = \{e\}$
c) A est distingué dans G.

Montrer qu'il existe alors un homomorphisme φ de B dans le groupe des automorphismes $\mathrm{Aut}(A)$ de A tel que l'on ait, pour tout $a \in A$ et pour tout $b \in B$:

$$ba = \varphi(a)b$$

Montrer que B est isomorphe à G/A.

2) Soient A et B deux groupes. On suppose qu'il existe un homomorphisme φ de B dans $\mathrm{Aut}(A)$. Montrer que l'ensemble produit $A \times B$, muni de la loi :

$$(a, b)(a', b') = (a\varphi(a'), bb')$$

est un groupe. Montrer que ce groupe est produit semi-direct de deux sous-groupes A' et B', respectivement isomorphes à A et B.

3) Donner un exemple de groupe qui soit produit semi-direct de deux sous-groupes sans être leur produit direct.

Exercice : Groupes non abélien d'ordre 8.
Soit G un groupe non abélien d'ordre 8.
1) Montrer que G possède un élément a d'ordre 4 et que cet élément engendre un sous-groupe distingué H.
2) Soit $T = G/H$ le groupe quotient et soit b un élément de G dont l'image dans G/H est le générateur. Montrer que $b^2 \in H$ et vaut soit e soit a^2.
3) Montrer que $b^{-1}ab \in H$ et vaut nécessairement a^3.
4) En déduire quels sont les groupes non abélien d'ordre 8 à isomorphisme près.

Exercice. Considérons dans $\mathfrak{S}_9$ la permutation $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 7 & 9 & 1 & 4 & 3 & 8 & 6 \end{pmatrix}$.
1) a) Décomposer la permutation α en produit de cycles disjoints, puis en produit de transpositions.
b) Quelle est la signature de α ? Quel est l'ordre de α ?
c) Déterminer α^{-1}.
d) Déterminer α^{26}.
2) Soient $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 2 & 1 & 9 & 5 & 6 & 8 \end{pmatrix}$ et $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 7 & 4 & 6 & 5 & 9 & 2 & 3 \end{pmatrix}$ dans $\mathfrak{S}_9$.
a) α et β sont-ils conjugués entre eux ? Idem pour α et γ.
b) Calculer $\alpha\beta\alpha^{-1}$. Les éléments α et β commutent-ils entre eux ? Idem pour α et γ.

Exercice. Soit $\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$) le groupe symétrique (resp. alterné) des permutations (resp. permutations paires) opérant sur l'ensemble $\{1, \ldots, n\}$.
1) Montrer que $\mathfrak{A}_5$ est le seul sous-groupe de $\mathfrak{S}_5$ d'ordre 60.
2) Considérons les deux cycles de $\mathfrak{S}_5$ suivants : $\sigma = (12345)$ et $\nu = (2345)$. Déterminer l'ordre de $\sigma\nu$. En déduire quel est le sous-groupe H de $\mathfrak{S}_5$ engendré par σ et ν.

Un exemple : Groupe n'admettant pas de sous-groupe d'ordre un diviseur de son ordre.
Montrer que le groupe alterné $\mathfrak{A}_4$ ne contient pas de sous-groupe d'ordre 6.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *William Burnside (1852-1927)*
Licence 3-ième année

Algèbre T.D. - 7

Exercice. Soit G un groupe fini agissant transitivement sur un ensemble fini X.

1) Que peut-on dire de $\mid X \mid$ par rapport à $\mid G \mid$?
2) Soit H un sous-groupe distingué de G. Montrer que le cardinal d'une orbite suivant H est un diviseur de $\mid X \mid$.

Exercice. Soit G un groupe fini $\neq \{e\}$ et H un sous-groupe de G. Soit p le plus petit premier divisant $\mid G \mid$ et soit k le nombre de classes de conjugaison. Montrer que si $k > \frac{|G|}{p}$ alors $Z(G) \neq \{e\}$.

Exercice. Soit G un groupe infini et H un sous-groupe de G, distinct de G et d'indice fini. Montrer que G n'est pas simple.
(on pourra considérer l'action de G sur G/H par translation à gauche : $g.aH = gaH$).

Exercice. Soit G un groupe fini, p le plus petit facteur premier de $\mid G \mid$ et H un sous-groupe d'indice p de G.
Montrer que H est distingué dans G.

Application aux groupes d'ordre pq, avec p et q premiers et $p < q$: le q-Sylow est distingué.

Exercice. Centre d'un p-groupe : théorème de Burnside.
Montrer que le centre d'un p-groupe non réduit à l'élément neutre est non réduit à l'élément neutre.
(Application de la formule des classes.)

Exercice.
1) Soit H un sous-groupe d'un groupe G et soit N l'intersection des conjugués de H, i.e.

$$N = \bigcap_{x \in G} xHx^{-1}$$

Montrer que N est le plus grand sous-groupe de H distingué dans G.
2) Montrer que si H est un sous-groupe de G d'indice fini n, alors l'intersection N des conjugués de H est d'indice un diviseur de $n!$ (remarquer que G/N est isomorphe à un sous-groupe de $\mathfrak{S}_n$).
3) En déduire que si un groupe simple G admet un sous-groupe d'indice fini $n > 1$, alors G est fini.

Exercice. De combien de manière différente le nombre 1000 peut-il s'écrire comme produit de trois entiers si l'on ne tient pas compte de l'ordre des facteurs ?

Exercice. Montrer que tout groupe fini est isomorphe à un sous-groupe d'un groupe alterné. (*Appliquer le théorème de Cayley.*).

Université de Toulon
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Année 2017/2018

Peter Ludwig Mejdell Sylow (1832-1918)

Algèbre T.D. - 8

Exercice. Soient G un groupe fini, p un nombre premier et P un p-sous-groupe de Sylow de G. Montrer que le nombre de p-sous-groupes de Sylow de G est égal à l'indice du normalisateur de P dans G.

Exercice. Soit p un diviseur premier de l'ordre de G. Montrer que s'il n'existe pas d'automorphisme intérieur d'ordre p dans $\mathrm{Int}(G)$, alors tout p-sous-groupe de Sylow de G est commutatif.

Exercice. Soit G un groupe fini et H un p-Sylow de G. Montrer que H est l'unique p-Sylow de G si et seulement si $H \triangleleft G$.

Exercice. Groupes d'ordre 6.
Montrer qu'un groupe d'ordre 6 est ou bien cyclique (i.e. isomorphe à $\mathbb{Z}/6\mathbb{Z}$), ou bien isomorphe au groupe symétrique $\mathfrak{S}_3$.

Exercice. Montrer que les 2-Sylow du groupe alterné $\mathfrak{A}_5$ sont isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Combien y en a-t-il ?

Exercice. Soit G un groupe fini d'ordre 50. Montrer que G n'est pas simple.

Exercice. Montrer qu'un groupe G d'ordre 200 contient un p-Sylow distingué dans G.

Exercice. Soit G un groupe simple d'ordre 168 *(voir un exemple de tel groupe plus loin)*. Trouver le nombre d'éléments d'ordre 7 de G.

Exercice. Soit G un groupe d'ordre 15. Montrer que G est cyclique.

Exercice. Soit G un groupe d'ordre pq, avec p et q premiers, $p < q$.
1) Montrer que G a un et un seul sous-groupe d'ordre q.
2) Montrer que si p ne divise pas $(q-1)$ alors G est cyclique d'ordre pq (exemple : $15, 35, 51 \ldots$).
3) Montrer que si p divise $(q-1)$ alors G n'est pas nécessairement cyclique.

Exercice. Soit G un groupe d'ordre > 2. On suppose que G admet un 2-Sylow cyclique H. Montrer que G n'est pas simple.
En déduire que si G est simple et d'ordre pair > 2 alors 4 divise l'ordre de G.

Exercice. Montrer qu'un groupe d'ordre 56 n'est pas simple (on déterminera le nombre d'éléments d'ordre 7).

Exercice. Montrer qu'un groupe d'ordre 48 n'est pas simple (on montrera qu'un tel groupe est égal au normalisateur de l'intersection de deux de ses 2-Sylow dans le cas où il en possède 3).

Exercice. Montrer qu'un groupe d'ordre 24 n'est pas simple (on fera agir un tel groupe supposé simple sur l'ensemble de ses 2-Sylow par conjugaison).

Exercice (Wilson par Sylow). En déterminant à la main le nombre d'éléments d'ordre p de $\mathfrak{S}_p$ et son nombre de p-Sylow (p premier), retrouver le théorème de Wilson qui dit que $(p-1)! \equiv -1 \bmod p$.

Exercice. Soit p un diviseur premier de l'ordre d'un groupe G. Montrer que s'il n'existe pas d'automorphisme intérieur d'ordre p dans $\mathrm{Int}(G)$, alors tout p-sous-groupe de Sylow de G est commutatif.

Exercice. Soit G un groupe abélien.
1) On note $\mathrm{Tor}(G)$ l'ensemble des éléments de G d'ordre fini. Montrer que $\mathrm{Tor}(G)$ est un sous-groupe de G.

On dit que G est un *groupe de torsion* si $\mathrm{Tor}(G) = G$, et que G est sans torsion si $\mathrm{Tor}(G) = \{0\}$.
2) Montrer que tout groupe fini est un groupe de torsion.
3) Montrer que $G/\mathrm{Tor}(G)$ est sans torsion.

Exercice. Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre 2250.

Exercice. Combien existe-t-il de groupes abéliens (à isomorphisme près) ayant même ordre que le groupe $(\mathbb{Z}/433\mathbb{Z})^*$? Combien parmi ceux-ci admettent un sous-groupe cyclique d'ordre 36 ?

Exercice. Montrer que les groupes $(\mathbb{Z}/11137\mathbb{Z})^*$ et $(\mathbb{Z}/21364\mathbb{Z})^*$ ont même ordre mais ne sont pas isomorphes.

Un exemple : groupe simple d'ordre 168.
Montrer que le groupe $PSL(3, \mathbb{F}_2)$ est un groupe simple d'ordre 168.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques *Niels Henrik Abel (1802-1829)*
Licence 3-ième année

Algèbre T.D. - 9

Exercice. Pour chacune des propriétés suivantes, trouver un exemple de groupe G vérifiant cette propriété, ou prouver qu'il n'en existe pas.
1) G est d'ordre 360, simple et abélien.
2) G est d'ordre 360, simple et non abélien.
3) G est d'ordre 360, ni simple ni abélien.
4) G est d'ordre compris entre 100 et 200, simple et abélien.

Exercice. Soit G un groupe simple d'ordre 60. Montrer que G ne possède pas de sous-groupe d'ordre 15 (par l'absurde : on fera agir un tel groupe sur l'ensemble des classes à droite modulo un tel sous-groupe par translation) . En déduire que G possède 20 éléments d'ordre 3 (on pourra faire agir notre groupe sur l'ensemble de ses 3-Sylow par conjugaison dans le cas où ces derniers sont au nombre de 4).

Exercice. Montrer qu'un sous-groupe simple de $\mathfrak{S}_n$ est nécessairement inclus dans $\mathfrak{A}_n$.

Exercice. On considère un groupe G, simple et d'ordre 60. Pour chaque nombre premier p, on note n_p le nombre de p-sous-groupes de Sylow (on dira encore p-Sylow) de G.
1) Calculer le cardinal d'un 2-Sylow de G, celui d'un 3-Slow et celui d'un 5-Sylow.
2) Pour quelles valeurs de p les p-Sylow de G sont-ils abéliens ?
3) Calculer le nombre n_5 de 5-Sylow et en déduire le nombre d'éléments d'ordre 5 dans G.
4) Donner un ensemble d'entiers $\mathbb{N}_3$ de cardinal aussi petit que vous pouvez pour lequel vous savez (et prouvez !) que $n_3 \in \mathbb{N}_3$. Même question pour un ensemble $\mathbb{N}_2$ tel que $n_2 \in \mathbb{N}_2$.

On admettra dans la suite que $n_2 = 5$.

Soit E_2 l'ensemble des 2-Sylow de G. Il a donc 5 éléments. On considère l'action ϕ de G sur l'ensemble E_2 par conjugaison :

$$\phi : (g, S) \longmapsto gSg^{-1} = \{gsg^{-1} \ , \ s \in S\}.$$

5) Combien y a-t-il d'orbites dans E_2 pour cette action ?
Montrer que le noyau de l'action ϕ n'est pas G tout entier.
L'action ϕ est-elle fidèle ?
6) En considérant ϕ comme un morphisme de G dans le groupe symétrique $\mathfrak{S}_5$, en déduire que G est isomorphe au groupe alterné $\mathfrak{A}_5$.

Exercice. Soit $\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$) le n-ième groupe symétrique (resp. alterné). On note $\mathcal{P}_{5,7}$ l'ensemble des parties à 5 éléments de l'ensemble $\{1, 2, 3, 4, 5, 6, 7\}$.
1) Quel est le cardinal de $\mathcal{P}_{5,7}$?

Si $\sigma \in \mathfrak{S}_7$ et $E = \{a_1, \ldots, a_5\} \subset \mathcal{P}_{5,7}$, on note $\sigma.E$ l'ensemble $\{\sigma(a_1), \ldots, \sigma(a_5)\}$.
2) Montrer que cela définit une action de $\mathfrak{S}_7$ sur $\mathcal{P}_{5,7}$. Est-elle fidèle ? Est-elle transitive ?

On note désormais G le stabilisateur dans $\mathfrak{S}_7$ de la partie $E_0 = \{3, 4, 5, 6, 7\}$ pour cette action.

3) Calculer le cardinal de G (sans utiliser le résultat du **4)**) et celui de $G \cap \mathfrak{A}_7$.

4) Montrer que G est isomorphe au produit $\mathfrak{S}_5 \times \mathbb{Z}/2\mathbb{Z}$. Le groupe G est-il abélien ? Est-il simple ? Est-il distingué dans $\mathfrak{S}_7$?

5) Combien y a-t-il d'éléments d'ordre 5 dans G ? Combien y a-t-il de 5-Sylow de G ?

6) Montrer que tout 2-Sylow de G est un 2-Sylow de $\mathfrak{S}_7$. La réciproque est-elle vraie ?

7) On note $\sigma = (1372546)$ et $\tau = (24)(3756)$. Les classes à droite de σG et τG sont-elles égales ? Si Σ désigne le groupe engendré par σ dans $\mathfrak{S}_7$, calculer le cardinal de $\Sigma \cap G$. Montrer qu'il existe un système de représentants des classes à droite de $\mathfrak{S}_7$ modulo G qui contient l'ensemble Σ.

Université de Toulon
U.F.R. de Sciences
Mathématiques Licence 3-ième année

Année 2017/2018

Deuxième partie

.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 1

Exercice 1. Groupe dérivé.

Soit G un groupe et $D(G)$ son groupe dérivé i.e. le sous-groupe de G engendré par les commutateurs $(xyx^{-1}y^{-1}, x, y \in G)$.

1) Montrer que G est abélien ssi $D(G) = \{e\}$.

2) Montrer que $D(G) \triangleleft G$.

3) Montrer que $G/D(G)$ est abélien. Montrer que c'est le plus grand quotient abélien de G, i.e. si $H \triangleleft G$ alors G/H abélien ssi $D(G) \subset H$.

4) Montrer que $D(\mathfrak{S}_3) = \mathfrak{A}_3$.

5) Montrer que $D(\mathfrak{A}_4) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

6) Soit $n \geq 5$. Montrer que les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

En déduire que

$$D(\mathfrak{A}_n) = D(\mathfrak{S}_n) = \mathfrak{A}_n.$$

7) Montrer que, si $n \geq 5$, $\mathfrak{S}_n$ n'admet que $\mathfrak{A}_n$ comme sous-groupe d'indice 2.

Exercice 2. Montrer, en étudiant ses sous-groupes, que le groupe alterné $\mathfrak{A}_4$ ne possède pas de sous-groupe d'ordre 6.

Exercice 3. Théorème de Cauchy.

Soit G un groupe fini et p un nombre premier divisant l'ordre de G. Le but de l'exercice est de montrer que G admet un élément d'ordre p (cela se fera par récurrence sur l'ordre de G).

1. Montrer qu'il suffit de montrer que G admet un élément d'ordre multiple de p.

2. Montrer le résultat si G est d'ordre p.

3. Soit k un entier. Supposons que pour tout $k' < k$, tout groupe d'ordre $k'p$ admette un élément d'ordre p.

Soit G un groupe d'ordre kp. Montrer le résultat tout d'abord dans le cas où G est abélien, puis, en déduire le résultat dans le cas non abélien en faisant agir G sur lui-même par conjugaison.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 2

Exercice 1. En utilisant le théorème de Sylow, montrer que le groupe alterné $\mathfrak{A}_4$ ne possède pas de sous-groupe d'ordre 6 (sinon, il n'aurait qu'un seul 3-Sylow).

Exercice 2. Montrer qu'un groupe d'ordre 50 n'est pas simple.

Exercice 3. Montrer qu'un groupe d'ordre 200 n'est pas simple.

Exercice 4. Montrer qu'un groupe d'ordre 24 n'est pas simple (on fera agir le groupe sur l'ensemble de ses 2-Sylow par conjugaison).

Exercice 5. Le but de cet exercice est de montrer qu'un groupe d'ordre 48 n'est pas simple, i.e. qu'il admet un sous-groupe distingué autre que le sous-groupe réduit à l'élément neutre et le groupe lui-même.
Soit G un groupe d'ordre 48.

1. Montrer que le nombre de 2-sous-groupes de Sylow de G est 1 ou 3.

2. Supposons que G ait un seul 2-sous-groupe de Sylow. Montrer qu'il est distingué dans G et conclure.

3. Supposons maintenant que G admette trois 2-sous-groupes de Sylow et soient H et K deux de ceux-ci.

3.1) Montrer que si S et T sont deux sous-groupes d'un groupe fini G alors :

$$\mid ST \mid = \frac{\mid S \mid \times \mid T \mid}{\mid S \cap T \mid}.$$

On pourra considérer l'application

$$\begin{array}{rccc} \phi : & S \times T & \longrightarrow & ST \\ & (s,t) & \longmapsto & st \end{array}$$

et montrer que $\phi^{-1}(st) = \{(sd, d^{-1}t) \mid d \in S \cap T\}$.

3.2) Montrer que si $\mid H \cap K \mid \leq 4$, on aboutit à une absurdité. En déduire l'ordre de $H \cap K$.

3.3) Montrer que $H \cap K \lhd H$ et $H \cap K \lhd K$.

3.4) On appelle normalisateur d'un sous-groupe T d'un groupe G l'ensemble

$$N_G(T) = \{x \in G \mid xTx^{-1} = T\}$$

Montrer que $N_G(T)$ est le plus grand sous-groupe de G dans lequel T soit distingué.

3.5) Soit N le normalisateur de $H \cap K$ dans G. Montrer que $HK \subset N$.

3.6) Montrer que $N = G$.

3.7) Conclure.

Exercice 6. Montrer qu'il n'existe aucun groupe dont le centre soit d'indice 69.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 3

Exercice 1. Déterminer à isomorphisme près tous les groupes d'ordre 6.
Quelle est la structure du groupe des automorphismes du groupe de Klein ?

Exercice 2 : Les groupes d'ordre 12.

1. Déterminer à isomorphisme près tous les groupes abéliens d'ordre 12.

2. Soit G un groupe non abélien d'ordre 12 et n_p le nombre de ses p-Sylow.

2.1 Montrer que si $n_3 = 4$ alors $n_2 = 1$. Montrer que le 2-Sylow est nécessairement non cyclique. Montrer que l'on trouve deux produits semi-directs isomorphes entre eux, de la forme :

$$V_4 \rtimes \mathbb{Z}/3\mathbb{Z}$$

où V_4 est le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

2.2 On suppose maintenant que G admet un unique 3-Sylow K. Montrer que selon que G/K soit cyclique ou non, G est isomorphe à un produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z} \rtimes V_4$.

3. Déterminer à isomorphisme près tous les groupes d'ordre 12. Reconnaître le groupe alterné $\mathfrak{A}_4$ et le groupe diédral D_6.

Exercice 3. Montrer qu'un groupe d'ordre 112 n'est pas simple.

Exercice 4. Soit G un groupe non abélien d'ordre p^3 et $Z(G)$ son centre. Montrer que :

$$G/Z(G) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Exercice 5. Soit G un groupe d'ordre $2p$ avec p premier impair. Déterminer le centre de G suivant qu'il est abélien ou non.

Exercice 6 : classes de conjugaison et simplicité de $\mathfrak{A}_5$.

Soit G un groupe fini. Si x et y sont deux éléments de G, on dit que x et y sont conjugués dans G (ou que x est conjugué à y dans G) s'il existe $g \in G$ tel que : $y = g^{-1}xg$. L'ensemble x^G des éléments conjugués à x dans G est appelé la classe de conjugaison de x dans G.

0. a) Si G est abélien, que dire des classes de conjugaison de G ?

b) Montrer que les transpositions $(1\quad 2)$ et $(1\quad 3)$ sont conjuguées dans le groupe symétrique $\mathfrak{S}_3$.

c) Montrer que les matrices $\begin{pmatrix} -2 & -3 & -4 \\ -1 & 0 & 0 \\ 2 & 2 & 3 \end{pmatrix}$ et $\begin{pmatrix} -9 & 72 & 52 \\ 1 & -5 & -4 \\ -3 & 20 & 15 \end{pmatrix}$ sont conjuguées (i.e. semblables !) dans le groupe linéaire $\mathrm{GL}_3(\mathbb{R})$.

1. Montrer que si $x, y \in G$, on a ou bien $x^G = y^G$, ou bien $x^G \cap y^G = \emptyset$. En déduire que l'ensemble des classes de conjugaison distinctes d'un groupe est une partition de ce groupe.

2. Montrer que si x et y sont conjugués dans G alors x^n et y^n sont conjugués dans G pour tout entier n et que x et y ont même ordre.

3. Soit x un élément de G. On définit le centralisateur de x dans G, noté $C_G(x)$, par :

$$C_G(x) = \{g \in G \mid xg = gx\}.$$

Montrer que $C_G(x)$ est un sous-groupe de G.

4. Soit $x \in G$. En considérant l'application f suivante :

$$\begin{array}{rccc} f: & x^G & \longrightarrow & G/C_G(x) \\ & gxg{-}1 & \longmapsto & gC_G(x) \end{array}$$

qui à tout conjugué gxg^{-1} de x dand G fait correspondre la classe à droite de g modulo le sous-groupe $C_G(x)$, montrer que

$$\sharp x^G = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

5. En déduire que si $x_1, \ldots, x_\ell$ sont des représentants de chaque classe de conjugaison de G alors on a la "formule des classes" suivante :

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x)]$$

où $Z(G)$ est le centre de G (i.e. les éléments de G qui commutent avec tous les éléments de G).

6. Déterminer les classes de conjugaison du groupe symétrique $\mathfrak{S}_4$. Retrouver l'ordre de $\mathfrak{S}_4$ par la formule des classes.

7. Idem pour le groupe alterné $\mathfrak{A}_4$, sous-groupe de $\mathfrak{S}_4$ constitué des permutations qui se décomposent en un nombre pair de transpositions.

8. En déduire tous les sous-groupes distingués de $\mathfrak{S}_4$.

9. En utilisant la même méthode que ci-dessus, montrer que le groupe alterné $\mathfrak{A}_5$ est simple (i.e. que les seuls sous-groupes distingués de $\mathfrak{A}_5$ sont $\{e\}$ et $\mathfrak{A}_5$ lui-même).

Exercice 7 : groupes simples d'ordre 60

Soit G un groupe simple d'ordre 60.

1. Montrer que G admet six 5-Sylow.

2. Soit S un 5-Sylow de G et $N_G(S)$ le normalisateur de S dans G. Quel est l'indice de $N_G(S)$ dans G ?

3. Montrer que :

$$\begin{array}{ccc} G \times G/N_G(S) & \longrightarrow & G/N_G(S) \\ (g, xN_G(S)) & \longmapsto & gxN_G(S) \end{array}$$

définit une action (à gauche) de G sur l'ensemble des classes à droite de G modulo $N_G(S)$, qui est transitive et fidèle. En déduire que G se plonge dans $\mathfrak{S}_6$; on notera J l'image de G via ce plongement.

4. Montrer que $J \subset \mathfrak{A}_6$.

5. Considérons l'action à gauche, transitive et fidèle, de $\mathfrak{A}_6$ sur l'ensemble des classes à droite de $\mathfrak{A}_6$ modulo J suivante :

$$\begin{array}{ccc} \mathfrak{A}_6 \times \mathfrak{A}_6/J & \longrightarrow & \mathfrak{A}_6/J \\ (g, xJ) & \longmapsto & gxJ \end{array}$$

On regarde $\mathfrak{A}_6$ comme le groupe des permutations paires sur l'ensemble $\mathfrak{A}_6/J = \{J = J_1, J_2, \ldots, J_6\}$.

Montrer que $J \subset \mathfrak{A}_5$.

6. Conclure que G est isomorphe à $\mathfrak{A}_5$.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 4

Groupes résolubles I

Exercice 1. Soit G un groupe fini. Montrer que les assertions suivantes sont équivalentes (un groupe vérifiant ces assertions est dit résoluble).

(i) il existe des sous-groupes $G_0, \ldots, G_n$ de G tels que :

$$G_n = \{e\} \lhd G_{n-1} \lhd \cdots \lhd G_0 = G$$

et G_i/G_{i+1} abélien $(0 \leq i \leq n-1)$.

(ii) il existe un entier s tel que $D^s(G) := D(D(\cdots(G))) = \{e\}$.

(iii) il existe des sous-groupes $G_0, \ldots, G_n$ de G tels que :

$$G_n = \{e\} \lhd G_{n-1} \lhd \cdots \lhd G_0 = G$$

et G_i/G_{i+1} cyclique d'ordre premier $(0 \leq i \leq n-1)$.

Exercice 2 : exemples de groupes résolubles et non résolubles.

1. Montrer que tout groupe abélien est résoluble.

2. Montrer que les groupes $\mathfrak{S}_3$, $\mathfrak{S}_4$ et D_4 sont résolubles.

3. Montrer que si un groupe est résoluble et simple alors il est cyclique d'ordre premier.

4. Montrer que $\mathfrak{S}_n$ n'est pas résoluble pour $n \geq 5$.

5. Montrer que tout p-groupe est résoluble.

Exercice 3. 1. Soit $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\}$ une série normale d'un groupe G (de longueur r).

Montrer que c'est une série de composition (de Jordan Holder) (i.e. que l'on ne peut pas intercaler de nouveaux termes et avoir toujours une série normale) si et seulement si ses quotients sont simples.

2. Soit G un groupe cyclique d'ordre p^n, p premier. Montrer que G admet une et une seule série de composition. Quels sont ses quotients ?

3. Soit $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Quels sont les sous-groupes de G ? Donner toutes les séries de composition de G.

4. Soient G un groupe, $N \triangleright G$, G' un groupe, $N' \triangleright G'$. Montrer que la série suivante est une série normale de $G \times G'$:

$$G \times G' \triangleright G \times N' \triangleright G \times \{e'\} \triangleright N \times \{e'\} \triangleright \{e\} \times \{e'\}.$$

Montrer que l'on peut, à l'aide de séries de compositoion de G et G', former une série de composition de $G \times G'$. Quels sont les quotients de la série ?

5. Montrer que tout groupe abélien fini admet une série de composition dont les quotients sont d'ordre premier.

Si G abélien est d'ordre $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, quel ensemble de quotients obtient-on ?

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 5

Groupes résolubles II

Exercice 1.
1. Montrer que tout groupe d'ordre pq, avec p et q premiers distincts, est résoluble.

2. Soit G un groupe d'ordre pqr, avec $p < q < r$ premiers. On se propose de montrer qu'un tel groupe n'est pas simple.

On suppose que G est simple.

a) Que peut-on dire des nombres de p-Sylow, q-Sylow et r-Sylow de G ?

b) Calculer le nombre d'éléments d'ordre r de G et donner une minoration des nombres d'éléments d'ordre p et d'ordre q de G.

c) Conclure.

3. En utilisant les résultats des deux premières questions, montrer que tout groupe d'ordre pqr, avec p, q, r premiers distincts, est résoluble.

Exercice 2. Montrer que tout groupe d'ordre p^2q avec p, q premiers, est résoluble.

Exercice 3. Soit G un groupe d'ordre > 2. Montrer que si G admet un 2-Sylow cyclique alors G n'est pas simple.

En déduire que si G est simple d'ordre pair différent de 2 alors 4 divise l'ordre de G.

Exercice 4. Simplicité des groupes d'ordre ≤ 100.

Montrer que si G est un groupe d'ordre n non premier et ≤ 100 et $\neq 60$ alors G n'est pas simple.

Exercice 5.

Soit $G = \mathrm{GL}_2(\mathbb{F}_2)$ le groupe des matrices carrées d'ordre 2 inversibles à coefficients dans le corps fini $\mathbb{F}_2$ à deux éléments.

1. a) Déterminer les éléments de G ainsi que leurs ordres.

b) Le groupe G est-il simple ?

c) Le groupe G est-il résoluble ?

2. Montrer que G est isomorphe à un produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

3. Soit $\mathcal{H}$ l'ensemble des 2-sous-groupes de Sylow de G. En faisant agir G sur $\mathcal{H}$ par conjugaison, montrer que G est isomorphe au groupe symétrique $\mathfrak{S}_3$.

Exercice 6 : Autour des groupes d'ordre 66.

On se donne un groupe G d'ordre 66 et on note n_p le nombre de ses p-Sylow.

1. Montrer que $n_{11} = 1$.

2. On s'intéresse maintenant au nombre de 3-Sylow de G.

2.1. En notant K le 11-Sylow de G et H un 3-Sylow de G, montrer que KH est un sous-groupe distingué de G et qu'il est cyclique.

2.2. Montrer que H est distingué dans G.

2.3. En conclure que l'on a nécessairement $n_3 = 1$.

3. Traiter le cas où G est abélien.

4. On suppose dorénavant que $n_2 \neq 1$. On note K le 11-Sylow de G, H le 3-Sylow de G et R un 2-Sylow de G.

4.1. Montrer que G est isomorphe au produit semi-direct suivant :

$$G \simeq \mathbb{Z}/33\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$$

avec φ morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/33\mathbb{Z})$.

4.2. Déterminer les éléments d'ordre 2 du groupe $\mathrm{Aut}(\mathbb{Z}/33\mathbb{Z})$.

4.3. En déduire les structures de produits semi-directs possibles pour G. Reconnaître parmi eux le groupe diédral D_{33} d'ordre 66.

4.4. Déterminer le nombre d'éléments d'ordre 2 de ces produits semi-directs. En déduire qu'ils sont non isomorphes entre eux. Reconnaître les groupes $D_{11} \times \mathbb{Z}/3\mathbb{Z}$ et $D_3 \times \mathbb{Z}/11\mathbb{Z}$.

5. Quels sont, à isomorphisme près, tous les groupes d'ordre 66 ? Quel est leur nombre de 2-Sylow à chacun ?

6. Un groupe d'ordre 66 est-il nécessairement résoluble ?

7. Montrer que tout groupe d'ordre 4422 est résoluble.

8. On s'intéresse aux plongements (i.e. morphisme injectifs de groupes) de certains groupes d'ordre 66 dans le groupe symétrique.

8.1. Montrer que tout groupe G d'ordre 66 peut se plonger dans le groupe symétrique $\mathfrak{S}_{66}$.

8.2. Montrer que $\mathbb{Z}/66\mathbb{Z}$ peut se plonger dans $\mathfrak{S}_{16}$ et dans aucun autre $\mathfrak{S}_n$ pour $n < 16$.

8.3. On fait agir le groupe diédral D_{33} sur l'ensemble de ses 2-Sylow par conjugaison.
(i) Montrer que le centre de D_{33} est trivial.
(ii) Montrer que D_{33} peut être engendré par deux éléments d'ordre 2.
(iii) En déduire que l'action est fidèle.
(iv) En déduire un plongement de D_{33} dans $\mathfrak{S}_{33}$.

Université de Toulon
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Année 2017/2018

Algèbre II - T.D. - 6

Idéaux premiers de $k[X,Y]$ et anneaux intégralement clos

Exercice 1 : idéaux premiers de $k[X,Y]$

Soit k un corps infini.

1. Soit (P) un idéal principal de $k[X,Y]$. Montrer que (P) n'est pas maximal (on pourra considérer l'idéal $(P, X-x)$ avec $x \in k$ bien choisi).
2. Montrer que si $F, P \in k[X,Y] \setminus \{0\}$, il existe Q et R dans $k[X,Y]$ et $a \in k[X] \setminus \{0\}$ tels que :
(i) $a(X)F(X,Y) = P(X,Y)Q(X,Y) + R(X,Y)$
(ii) $\deg_Y(R) < \deg_Y(P)$.
(on pourra travailler dans l'anneau euclidien $k(X)[Y]$).

Soit m un idéal premier non principal de $k[X,Y]$.

3. Montrer que m contient deux polynômes $P(X)$ et $Q(Y)$ irréductibles (on pourra considérer un polynôme de degré minimal en X parmi les polynômes de m de degré minimal en Y).
4. En déduire qu'alors m est maximal.

On pourra considérer l'isomorphisme suivant :

$$k[X,Y]/m \simeq (k[X]/(P))[Y]/\bar{m}$$

où $\bar{m}$ est l'image de m par la surjection canonique de $k[X][Y]$ sur $(k[X]/(P))[Y]$.
5. Si k est algébriquement clos, montrer que m est de la forme :

$$m = (X-a, Y-b).$$

6. Donner tous les idéaux premiers de $k[X,Y]$.

Exercice 2 : anneaux intégralement clos

On considère un anneau unitaire commutatif B et A un sous-anneau de B. Un élément x de B est dit *entier* sur A s'il est racine d'un polynôme unitaire à coefficients dans A, i.e. s'il existe $a_0, \ldots, a_{n-1} \in A$ tels que :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

L'ensemble $F_B(A)$ des éléments de B entiers sur A est un sous-anneau de B contenant A, appelé la fermeture intégrale de A dans B. Si $F_B(A) = B$ on dit que B est entier sur A. Si $F_B(A) = A$ on dit que A est intégralement fermé dans B. Si A est intègre et si A est intégralement fermé dans son corps des fractions, on dit que A est intégralement clos.

I

1. L'élément $\sqrt{2} \in \mathbb{R}$ est-il entier sur $\mathbb{Z}$?

2. Si B est entier sur A et si I est un idéal de B et $J = I \cap A$, montrer alors que B/I est entier sur A/J.

3. Montrer que tout corps est un anneau intégralement clos.

4. Montrer que l'anneau des polynômes $K[X]$ où K est un corps est intégralement clos.

On montre de même que tout anneau factoriel (et donc tout anneau principal) est intégralement clos.

II

Soit $d \in \mathbb{Z}$ un entier relatif sans facteur carré et soit

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d}, a, b \in \mathbb{Q}\}.$$

Soit $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$; on définit le conjugué $\bar{x}$ de x par $\bar{x} = a - b\sqrt{d}$, la trace $T(x)$ de x par $T(x) = x + \bar{x} = 2a$ et la norme $N(x)$ de x par $N(x) = x\bar{x} = a^2 - db^2$.

1. Montrer que $\mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{R}$.

2. a) Montrer que l'application de $\mathbb{Q}(\sqrt{d})$ dans lui-même qui à tout élément associe son conjugué est un automorphisme de corps.

b) Montrer que l'application trace $T : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}$ qui à tout élément associe sa trace est une forme linéaire du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{d})$.

c) Montrer que l'application norme $N : \mathbb{Q}(\sqrt{d})^* \longrightarrow \mathbb{Q}^*$ qui à tout élément associe sa norme est un morphisme de groupes.

3. Montrer que pour qu'un élément de $\mathbb{Q}(\sqrt{d})$ soit entier sur $\mathbb{Z}$ il faut et il suffit que sa trace et sa norme soient dans $\mathbb{Z}$.

4. Soit $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.

a) Montrer que si x est entier sur $\mathbb{Z}$ alors $d(2b)^2 \in \mathbb{Z}$ et $2b \in \mathbb{Z}$.

b) Montrer que si $d \equiv 2 \bmod 4$ ou si $d \equiv 3 \bmod 4$ alors x est entier sur $\mathbb{Z}$ si et seulement si a et b sont dans $\mathbb{Z}$.

c) Montrer que si $d \equiv 1 \bmod 4$ alors x est entier sur $\mathbb{Z}$ si et seulement si $2a$ et $2b$ sont des entiers de $\mathbb{Z}$ de même parité.

d) Montrer que si $d \equiv 1 \bmod 4$ alors l'anneau $\mathbb{Z}(\sqrt{d}) = \{a + b\sqrt{d}, a, b \in \mathbb{Z}\}$ n'est pas intégralement clos.

III

Soient A un anneau unitaire commutatif intègre et $A[X]$ l'anneau des polynômes à une indéterminée à coefficients dans A.

1. a) Montrer que toute intersection d'anneaux intégralement clos A_i contenus dans un même anneau intègre B est intégralement clos.

b) En déduire que si $A[X]$ est intégralement clos alors A est intégralement clos.

2. On suppose que A est intégralement clos et on note K son corps des fractions. *On veut montrer qu'alors $A[X]$ est intégralement clos.*

On admet que pour tout corps K, il existe un corps Ω ayant les propriétés suivantes :
(i) $\Omega \supset K$
(ii) Tout polynôme $P \in \Omega[X]$ se factorise en un produit de polynômes de degré 1.

a) Montrer que si h est un polynôme unitaire de $K[X]$ tel que toutes ses racines dans Ω sont entières sur A alors $h \in A[X]$. En déduire que si f et g sont deux polynômes unitaires de $K[X]$ tels que $fg \in A[X]$ alors f et g appartiennent à $A[X]$.

b) Soit $h \in \mathrm{Frac}(A[X])$, le corps des fractions de $A[X]$, tel que h soit entier sur $A[X]$.

(i) Montrer que $h \in K[X]$.

(ii) Soit $Q \in (A[X])[T]$, $Q = T^n + f_{n-1}T^{n-1} + \cdots + f_0$, avec $f_i \in A[X]$, tel que $Q(h) = 0$.
Posons $h_1 = h - X^r$ pour un certain entier $r > \deg h$ et considérons le polynôme

$$Q(T + X^r) = T^n + g_{n-1}T^{n-1} + \cdots + g_0$$

où $g_i \in A[X]$, $i = 0, \ldots, n-1$.

Montrer que le polynôme g_0 de $A[X]$ est unitaire pour r assez grand.

En déduire (en utilisant III 2.a) que $-h_1 \in A[X]$.

Conclure que $A[X]$ est intégralement clos.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 7

Anneaux intègres, euclidiens, principaux

Exercice 1 : racines d'un polynôme

Soit A un anneau commutatif unitaire. Démontrer l'équivalence des propositions suivantes :
(i) A est intègre.
(ii) Tout polynôme de $A[X]$ de degré $n \geq 1$ a au plus n racines dans A.
(iii) Tout polynôme linéaire non nul $Q(X) = aX$ de $A[X]$ admet au plus une racine dans A.

Exercice 2 : une équation diophantienne.

1. Montrer que $\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien.

2. En déduire que les seules solutions entières de l'équation

$$x^2 + 2 = y^3$$

sont les deux couples $(5, 3)$ et $(-5, 3)$.

Exercice 3 : anneau principal non euclidien.

1. a) Montrer que si A est un anneau euclidien alors il existe $x \in A \setminus A^*$ tel que la restriction à $A^* \cup (0)$ de la projection canonique de A sur $A/(x)$ soit surjective (et alors $A/(x)$ est un corps).

b) Considérons l'anneau $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Déterminer A^*. En déduire que A n'est pas euclidien.

2. On admet que $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est muni d'une pseudo division euclidienne *i.e.* si $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que
(i) $r = 0$ ou $N(r) < N(b)$ (où $N(z) = z\bar{z}$)
(ii) $a = bq + r$ ou $2a = bq + r$.

a) Montrer que l'idéal (2) est maximal dans A.

b) Soit I un idéal non réduit à $\{0\}$ de A et a un élément non nul de I tel que $N(a)$ soit minimal. Si $I \neq (a)$, considérer $x \in I \setminus (a)$ et montrer qu'il existe $q \in A$ tel que $2x = aq$, puis qu'il existe $a' \in A$ tel que $x = a'q$. Montrer que $a' \in I$. Conclure que A est principal.

(Autre exemple : l'anneau $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$.)

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 8

Anneaux factoriels

Exercice 1. On rappelle qu'un anneau factoriel A est un anneau intègre dans lequel :

(E) tout élément non nul se décompose en produit d'irréductibles, *i.e.*

$$\forall a \in A \setminus \{0\}, a = up_1 \dots p_r \text{ avec } u \in A^* \text{ et } p_1, \dots, p_r \text{ irreductibles}$$

et

(U) cette décomposition est unique, à permutation près et à des inversibles près, *i.e.*

$$a = up_1 \dots p_r = vq_1 \dots q_s \Rightarrow r = s \text{ et } \exists \sigma \in \mathcal{S}_r \text{ tel que } p_i \text{ et } q_{\sigma(i)} \text{ associes.}$$

Soit A un anneau intègre vérifiant (E). Montrer que les conditions suivantes sont équivalentes :

(1) A vérifie (U).
(2) Lemme d'Euclide : Si p est irréductible et $p \mid ab$ alors $p \mid a$ ou $p \mid b$.
(3) p irréductible si et seulement si p est premier (*i.e.* si l'idéal (p) est premier et non nul)
(4) Théorème de Gauss : si $a \mid bc$ et si a est premier avec b alors $a \mid c$.

Exercice 2. Montrer que l'anneau

$$A = \mathbb{Z}[i\sqrt{5}]$$

n'est pas factoriel.

Exercice 3. On rappelle qu'un anneau de Dedekind est un anneau intègre, intégralement clos dans lequel tout idéal est de type fini et tout idéal premier non nul est maximal.

On rappelle également que dans un tel anneau, tout idéal est produit d'idéaux premiers.

1. Montrer que si les idéaux maximaux d'un anneau de Dedekind sont principaux, alors l'anneau est principal.

2. Soit $\mathcal{P}$ un idéal premier non nul d'un anneau factoriel. Montrer qu'il existe un élément p premier tel que $p \in \mathcal{P}$.

3. En déduire que si un anneau de Dedekind est factoriel, alors il est principal.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 9

Corps finis

Exercice 1.
1. Soit K un corps fini. Montrer qu'il existe un nombre premier p et un entier n tel que :

$$\sharp K = p^n.$$

Que représentent p et n ?

2. Soit K un corps fini de cardinal $q = p^n$. Montrer que pour tout $x \in K$, on a :

$$x^q - x = 0.$$

3. En déduire que pour tout nombre premier p et tout entier $n > 0$ il existe, à isomorphisme près, un unique corps fini à p^n éléments.

On note ce corps $\mathbb{F}_{p^n}$.

Exercice 2. Montrer qu'un corps fini n'est pas algébriquement clos.

Exercice 3. Ecrire le treillis des sous-corps du corps fini $\mathbb{F}_{2^{30}}$.

Exercice 4.
1. a) Montrer que $P(X) = X^2 + 1 \in \mathbb{F}_3[X]$ est un polynôme irréductible sur $\mathbb{F}_3$.

b) On pose $\mathbb{F}_9 = \mathbb{F}_3[X]/(P(X))$ et soit α une racine de $P(X)$ dans un corps de décomposition de $P(X)$ sur $\mathbb{F}_3$. Ecrire tous les éléments de $\mathbb{F}_9$.

2. a) Montrer que les polynômes $P_1(X) = X^2+X+2$ et $P_2(X) = X^2+2X+2$ sont irréductibles sur $\mathbb{F}_3$.

b) Calculer $Q(X) = P_1(X)P_2(X)$.

c) Soit ζ une racine de $P_1(X)$. Montrer que ζ est une racine primitive 8ème de l'unité sur $\mathbb{F}_3$.

En déduire un écriture des éléments de $\mathbb{F}_9$ en fonction de *zeta*.

d) Retrouver la forme de $\mathbb{F}_9$ de la question 1 à l'aide de cette dernière écriture (on pourra calculer $P_1(1+\alpha)$ où $\alpha^2 + 1 = 0$).

Exercice 5. Soit K un corps commutatif de caractéristique $p > 0$. On considère l'application

$$\begin{array}{rccc} F: & K & \longrightarrow & K \\ & x & \longmapsto & x^p \end{array}$$

1. Montrer que F est un homomorphisme de corps appelé homomorphisme de Frobenius.

2. Montrer que si K est fini alors F est un automorphisme de K.

3. Montrer que si $K = \mathbb{F}_p$ alors F est l'identité de K.

Exercice 6. Soit $q = p^n$ avec p premier et n entier non nul. On note Γ l'ensemble des carrés de $\mathbb{F}_q$, *i.e.*

$$\Gamma = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\},$$

et $\Gamma^* = \Gamma \cap \mathbb{F}_q^*$.

1. Montrer que si $p = 2$ alors $\Gamma = \mathbb{F}_q$.

On suppose désormais que $p > 2$.

2. a) Montrer que $\sharp\Gamma = \frac{q+1}{2}$ et $\sharp\Gamma^* = \frac{q-1}{2}$.

b) En déduire que l'on a :

$$x \in \Gamma^* \iff x^{\frac{q-1}{2}} = 1.$$

c) En déduire que

$$-1 \in \Gamma^* \iff q \equiv 1 \bmod 4.$$

d) Application : montrer qu'il existe une infinité de nombres premiers de la forme $4m + 1$ (considérer un facteur premier de $(n!)^2 + 1$ pour un entier n donné).

Exercice 7.

1. Existe-t-il un corps à 343 éléments ?

2. Soit a un élément de $\mathbb{F}_7$. Pour quelles valeurs de a le polynôme $X^3 - a$ est-il irréductible dans $\mathbb{F}_7[X]$?

En déduire que $K = \mathbb{F}_7[X]/(X^3 - 2)$ est un corps.

3. Quels sont les ordres possibles d'un élément du groupe multiplicatif K^* ?

Quel est l'ordre de la classe x de X dans K^* ?

4. Trouver un élément y d'ordre 19 dans K^*, de la forme $a + bx$, avec a et b dans $\mathbb{F}_7$.

5. En déduire un générateur μ du groupe multiplicatif K^*. Déterminer le polynôme minimal de μ sur K.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 10

Polynômes irréductibles

Exercice 1. Montrer que $P(X) = X^3 - 3X + 1$ est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

Exercice 2. Montrer que $P(X) = 199X^3 + 1998X^2 + X + 2001$ est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

Exercice 3. Soit $a \in \mathbb{Z}$ dont la décomposition en facteurs premiers est $a = \varepsilon p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et avec l'un des α_i égal à 1. Montrer que

$$P(X) = X^n - a$$

est irréductible sur $\mathbb{Z}$.

Exercice 4. Montrer que $P(X, Y) = Y^2 - X^3 + X$ est irréductible dans $\mathbb{R}[X, Y]$.

Exercice 5. Montrer que $P(X) = X^p - X - 1$ est irréductible sur $\mathbb{F}_p$ (p premier). En déduire que pour tout nombre premier p, le polynôme $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

Exercice 6. On veut montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais est réductible sur $\mathbb{F}_p$ pour tout nombre premier p.

1. Montrer que $X^4 + 1$ est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

2. Soit $P(X) \in k[X]$ un polynôme de degré n sur un corps k.

Montrer que $P(X)$ est irréductible sur k si et seulement si $P(X)$ n'a pas de racine dans les extensions K de k telles que $[K : k] \leq \frac{n}{2}$.

3. Montrer que pour tout nombre premier $p > 2$, on a :

$$8 \mid p^2 - 1.$$

En déduire que $\mathbb{F}_{p^2}^*$ contient un élément d'ordre 8 pour tout premier $p > 2$.

4. En déduire que $P(X) = X^4 + 1$ est réductible sur $\mathbb{F}_p$ pour tout p premier.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 11

Eléments algébriques

Exercice 1. Polynôme minimal.

1. Montrer que $\alpha =^3 \sqrt{2}$ est algébrique (sur $\mathbb{Q}$) et déterminer son polynôme minimal (sur $\mathbb{Q}$).

2. Idem pour $\beta = \cos(\frac{\pi}{9})$.

3. Idem pour $\gamma = \sqrt{2} + \sqrt{3}$.

Exercice 2. Existence de nombres transcendants sans en exhiber aucun (Cantor, 1874)

1. Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme de $\mathbb{Z}[X]$. On définit sa hauteur par :

$$h(P) = n + \mid a_0 \mid + \cdots + \mid a_n \mid .$$

Montrer qu'il n'y a qu'un nombre fini de polynômes dans $\mathbb{Z}[X]$ de hauteur donnée h.

2. Montrer que l'ensemble des nombres algébriques (*i.e.* des nombres complexes algébriques sur $\mathbb{Q}$) est un ensemble dénombrable.

En déduire l'existence de nombres transcendants.

Exercice 3. Degré et base.

1. Quels sont les degrés des extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$?

Donner une base de ces $\mathbb{Q}$-espaces vectoriels.

2. Quel est le degré de $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$ sur $\mathbb{Q}(\sqrt[3]{2})$, sur $\mathbb{Q}(\sqrt{2})$ et sur $\mathbb{Q}$?

Donner une base de $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$ sur $\mathbb{Q}$.

Exercice 4. Cyclotomie.

Soient k un corps, $n \in \mathbb{N} \setminus \{0\}$ un entier premier à la caractéristique de k et $P_n(X)$ le polynôme suivant :

$$P_n(X) = X^n - 1.$$

1. Montrer que $P_n(X)$ n'a que des racines simples.

2. On note $\mu_n(k)$ l'ensemble des racines n-ièmes de l'unité dans k :

$$\mu_n(k) = \{\zeta \in k \mid \zeta^n = 1\},$$

et K_n un corps de décomposition de P_n sur k.

Montrer que $\mu_n(k) \simeq \mathbb{Z}/d\mathbb{Z}$ pour un certain diviseur d de n.

3. On note $\mu_n^*(K_n)$ l'ensemble des racines primitives n-ième de l'unité de K_n, *i.e.*

$$\mu_n^*(K_n) = \{\zeta \in K_n \mid \zeta^n = 1 \text{ et } \zeta^d \neq 1 \text{ pour } d < n\}.$$

Montrer que :

$$\sharp(\mu_n^*(K_n)) = \varphi(n)$$

où φ est la fonction indicatrice d'Euler.

4. On définit le n-ième polynôme cyclotomique sur k, noté $\Phi_{n,k}(X) \in k[X]$ par :

$$\Phi_{n,k}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta).$$

4.1 Montrer que :

$$X^n - 1 = \prod_{d|n} \Phi_{d,k}(X).$$

4.2. Montrer que si p est premier alors :

$$\Phi_{p,k} = X^{p-1} + \cdots + X + 1.$$

4.3 Calculer $\Phi_{n,k}(X)$ pour $1 \leq n \leq 8$.

4.4. Montrer que $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ (il est même irréductible !).

5. Soit ζ_n une racine primitive n-ième de l'unité dans $\mathbb{R}$.

5.1. Montrer que $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne.

5.2. Calculer $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ et $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Université de Toulon **Année 2017/2018**
U.F.R. de Sciences
Mathématiques
Licence 3-ième année

Algèbre II - T.D. - 12

Théorie de Galois

Exercice 1.

Soit L un corps de décomposition sur $\mathbb{Q}$ du polynôme $P(X) = X^3 - 2$ et $G = \mathrm{Gal}(L/\mathbb{Q})$.

1) Déterminer $[L : \mathbb{Q}]$.

2) Ecrire les éléments de G.

3) Déterminer la structure de G.

4) Déterminer les corps des invariants (corps fixes) des sous-groupes de G.

5) Ecrire le treillis des sous-groupes de G ainsi que celui des extensions intermédiaires de $L/\mathbb{Q}$..

6) Quels sont les corps intermédiaires N de $L/\mathbb{Q}$ tels que $N/\mathbb{Q}$ soit galoisienne ?

Exercice 2.

On considère le polynôme $P(X) = X^4 - 2$ de $\mathbb{Q}[X]$ et on s'intéresse au groupe de Galois de son corps de décomposition sur $\mathbb{Q}$.

1) Notons $\alpha =^4 \sqrt{2} = 2^{1/4}$ la racine quatrième réelle et positive de 2.

Ecrire $P(X)$ comme produit de facteurs de degré un en fonction de α dans $\mathbb{R}[X]$.

Quel est le corps de décomposition K de $P(X)$ sur $\mathbb{Q}$?

L'extension $K/\mathbb{Q}$ est-elle galoisienne ?

2) Déterminer le polynôme minimal de i sur $\mathbb{Q}(\alpha)$, où i est une racine carrée de -1 dans $\mathbb{R}$.

Quel est le polynôme minimal de α sur $\mathbb{Q}$?

En déduire le degré de l'extension $K/\mathbb{Q}$.

3) Montrer qu'il existe des $\mathbb{Q}$-automorphismes σ et τ de K tels que $\sigma(i) = i$, $\sigma(\alpha) = i\alpha$ et $\tau(i) = -i$, $\tau(\alpha) = \alpha$.

En déduire, en fonction de σ et τ, tous les $\mathbb{Q}$-automorphismes de K.

4) Soit $G = \mathrm{Gal}(K/\mathbb{Q})$ le groupe formé de ces $\mathbb{Q}$-automorphismes. A quel groupe est-il isomorphe ?

5) Déterminer en fonction de σ et τ tous les sous-groupes de G et dire à quels groupes ils sont isomorphes.

6) Ecrire le treillis des sous-groupes de G. En déduire celui des extensions intermédiaires de $K/\mathbb{Q}$.

7) Expliciter ces corps intermédiaires.

8) Quelles sont les extensions galoisiennes de $\mathbb{Q}$ contenues dans K ?

9) Déterminer le groupe de Galois de $\mathbb{Q}(i, \sqrt{2})$ sur $\mathbb{Q}$.

Exercice 3 : théorème de d'Alembert (par Galois et Sylow).

On considère le corps $\mathbb{R}$ des réels et le corps $\mathbb{C} = \mathbb{R}(i)$ des complexes. On veut montrer que $\mathbb{C}$ est algébriquement clos, *i.e.* que tout polynôme non constant à coefficients complexes est scindé sur $\mathbb{C}$.

1. Montrons tout d'abord deux résultats préliminaires.

1.1. Montrer que tout polynôme à coefficients réels de degré impair admet au moins une racine dans $\mathbb{R}$. En déduire que la seule extension de degré impair de $\mathbb{R}$ est $\mathbb{R}$ lui-même.

1.2. Montrer que tout complexe est le carré d'un complexe. En déduire que $\mathbb{C}$ n'admet pas d'extension de degré 2.

2. Soit $P(X) = a_d X^d + \cdots + a_1 X + a_0 \in \mathbb{C}[X]$ un polynôme non nul et posons $\bar{P}(X) = \bar{a}_d X^d + \cdots + \bar{a}_1 X + \bar{a}_0$ et $Q(X) = (X^2+1)P(X)\bar{P}(X)$, où $\bar{a}_i$ est le conjugué du complexe a_i.

2.1. Montrer que $Q(X) \in \mathbb{R}[X]$.

2.2. Soit N un corps de décomposition de $Q(X)$ sur $\mathbb{R}$.

a) Montrer que l'extension $N/\mathbb{R}$ est galoisienne.

b) On note $G = \mathrm{Gal}(N/\mathbb{R})$ le groupe de Galois de $N/\mathbb{R}$. Montrer que G est d'ordre pair.

c) Montrer que l'ordre de G est une puissance de 2 (on pourra considérer le 2-Sylow de G).

d) Montrer que G est d'ordre 2 (on pourra considérer un sous-groupe d'indice 2 de $\mathrm{Gal}(N/\mathbb{C})$).

e) En déduire que $N = \mathbb{C}$. Conclure.

Exercice 4 : polynôme non résoluble par radicaux.

On considère le polynôme de $\mathbb{Q}[X]$ suivant :

$$P(X) = X^5 - 4X + 2.$$

1. Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$.

2. Montrer que $P(X)$ admet exactement deux zéros non réels.

3. Soient N un corps de décomposition de $P(X)$ sur $\mathbb{Q}$ et $G = \mathrm{Gal}(N/\mathbb{Q})$.

3.1. Montrer que G admet un élément d'ordre 5 et un élément d'ordre 2.

3.2. En identifiant G à un sous-groupe du groupe symétrique $\mathfrak{S}_5$, montrer que l'on peut se ramener à :

$$s = (\,1 \quad 2 \quad 3 \quad 4 \quad 5\,) \in G \;\text{ et }\; t = (\,1 \quad 2\,) \in G,$$

puis en déduire que $G = \mathfrak{S}_5$.

4. On dit qu'un polynôme de $\mathbb{Q}[X]$ est résoluble par radicaux s'il existe une extension L de $\mathbb{Q}$, contenant un corps de décomposition N du polynôme, définie par une tour $(K_i)_{0\leq i\leq n}$ telle que $K_0 = \mathbb{Q}$, K_{i+1}/K_i soit une extension cyclique (*i.e.* galoisienne à groupe de Galois cyclique) pour $1 \leq i \leq n-1$ et $L = K_n$ avec $L/\mathbb{Q}$ extension normale.

Montrer que si un polynôme $Q(X) \in \mathbb{Q}[X]$ est résoluble par radicaux alors le groupe de Galois $\mathrm{Gal}(N/\mathbb{Q})$ d'un corps de décomposition N de $Q(X)$ sur $\mathbb{Q}$ est un groupe résoluble.

5. En déduire que le polynôme $P(X)$ n'est pas résoluble par radicaux.

Exercice 5 : groupes abéliens comme groupes de Galois sur $\mathbb{Q}$.

On se propose de montrer dans ce problème que tout groupe abélien fini est groupe de Galois sur $\mathbb{Q}$.

I

Pour tout entier $m \geq 1$, on note $\Phi_m(X)$ le m-ième polynôme cyclotomique :

$$\Phi_m(X) = \prod_{\zeta}(X - \zeta)$$

où ζ parcourt les racines primitives m-ièmes de l'unité dans $\mathbb{C}$.

On admettra que $\Phi_m(X)$ est un polynôme irréductible de $\mathbb{Z}[X]$ et on rappelle que l'on a :

$$X^m - 1 = \prod_{d|m} \Phi_d(X).$$

1. Soient n et m des entiers et p un nombre premier tel que p divise $\Phi_m(n)$. On veut montrer que l'on a, ou bien $p \equiv 1 \bmod m$, ou bien p divise m.

a) Montrer que l'ordre μ de la classe de n modulo p divise m (i.e. $n^m \equiv 1 \bmod p$).

b) Si l'on suppose que $\mu = m$, montrer que $p \equiv 1 \bmod m$.

c) Supposons que $\mu < m$. Montrer que la classe de n est racine de $\Phi_d(X)$ modulo p pour un certain $d < m$, puis qu'elle est au moins racine double de $X^m - 1$ modulo p.
En déduire que p divise m.

2. On veut maintenant montrer, en utilisant la question 1, l'existence d'une infinité de nombres premiers dans certaines progressions arithmétiques.

a) Considérons un entier α tel que $\Phi_m(m^\alpha) \neq 1$, et soit p_1 un diviseur premier de $\Phi_m(m^\alpha)$. Montrer que

$$p_1 \equiv 1 \bmod m.$$

b) En déduire que pour tout entier $m \neq 0$, l'ensemble des nombres premiers p tels que $p \equiv 1 \bmod m$ est infini.

II

1. Soient n un entier et ζ_n une racine primitive n-ième de l'unité.

a) Montrer que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne.

b) Déterminer le degré $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

c) Si $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, montrer qu'il existe un entier a_σ premier avec n tel que $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$.

d) En considérant l'application Ψ suivante :

$$\begin{array}{rccc} \Psi : & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ & \sigma & \longmapsto & a_\sigma + n\mathbb{Z} \end{array}$$

montrer que :

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*.$$

2. Soit G un groupe abélien fini. On rappelle qu'il existe alors des entiers non nuls $m_1, \ldots, m_r$ tels que :

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}.$$

a) Montrer (en utilisant I) qu'il existe des nombres premiers impairs distincts $p_1, \ldots, p_r$ tels que : $p_i \equiv 1 \bmod m_i$ pour tout $i \in \{1, \ldots, r\}$.

b) On pose $n = p_1 \cdots p_r$ et $H = \big(m_1\mathbb{Z}/(p_1 - 1)\mathbb{Z}\big) \times \cdots \times \big(m_r\mathbb{Z}/(p_r - 1)\mathbb{Z}\big)$.
Montrer que le groupe de Galois de $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ contient un sous-groupe H' isomorphe à H.
Montrer, pour conclure, que G est le groupe de Galois d'une extension galoisienne de $\mathbb{Q}$.

$$\int\int\int$$