L'EVARISTE

Examen du matin

Durée : 2 heures

ALBERTSCHOOL D E Shaw & Co

Chaque section contient des questions de difficulté croissante. Il est autorisé de sauter certaines questions si vous êtes bloqué.

I - Mise en route

1. a) Résoudre $ax + b = 0$ $(a, b \in \mathbb{R},\ a \neq 0)$.

1pt

La solution de l'équation est $x = -\frac{b}{a}$.

b) Utiliser votre formule pour résoudre $5x + 7 = 0$.

1pt

La solution de l'équation est $x = -\frac{7}{5}$.

2. a) En complétant le carré, résoudre $ax^2 + bx + c = 0$ $(a, b, c \in \mathbb{R},\ a \neq 0)$.

8pts

$$
\begin{aligned}
ax^2 + bx + c &= 0 \\
x^2 + \frac{b}{a}x + \frac{c}{a} &= 0 \\
x^2 + \frac{b}{a}x &= -\frac{c}{a} \\
x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 &= -\frac{c}{a} + \left(\frac{b}{2a}\right)^2 \quad \text{(complétion du carré)} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x + \frac{b}{2a} &= \pm\frac{\sqrt{b^2 - 4ac}}{2a} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\end{aligned}
$$

b) Utiliser votre formule, ou toute autre méthode, pour résoudre les équations suivantes :

i) $x^2 + x - 6 = 0$

2pts

$x = -3$ ou $x = 2$

ii) $x^2 - 24x + 143 = 0$

2pts

$x = 11$ ou $x = 13$

iii) $x^4 - 5x^2 + 6 = 0$

2pts

$x = \pm\sqrt{2}$ ou $x = \pm\sqrt{3}$

iv) $(e^x)^2 - 5e^x + 6 = 0$

2pts

$x = \ln(2)$ ou $x = \ln(3)$

3. On considère maintenant l'équation $ax^3 + bx^2 + cx + d = 0$ $(a, b, c, d \in \mathbb{R},\ a \neq 0)$. Justifier que cette équation peut être ramenée à $x^3 + a'x^2 + b'x + c' = 0$.

3pts

We start with the cubic equation

$$ax^3 + bx^2 + cx + d = 0, \quad a \neq 0.$$

We can divide the entire equation by a to simplify it :

$$\frac{ax^3}{a} + \frac{bx^2}{a} + \frac{cx}{a} + \frac{d}{a} = 0,$$

which gives

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0.$$

If we set

$$a' = \frac{b}{a}, \quad b' = \frac{c}{a}, \quad c' = \frac{d}{a},$$

the equation becomes

$$x^3 + a'x^2 + b'x + c' = 0.$$

Thus, any cubic equation with leading coefficient $a \neq 0$ can be rescaled to a cubic equation with leading coefficient 1.

4. En utilisant $x = y - \frac{a'}{3}$, montrer que l'équation ci-dessus est équivalente à $y^3 + py + q = 0$, en exprimant p et q en fonction de a', b', c'.

3pts

We start from the cubic equation in the form

$$x^3 + a'x^2 + b'x + c' = 0.$$

We make the substitution

$$x = y - \frac{a'}{3}.$$

Then

$$x^3 = \left(y - \frac{a'}{3}\right)^3 = y^3 - a'y^2 + \frac{a'^2}{3}y - \frac{a'^3}{27},$$

$$a'x^2 = a'\left(y - \frac{a'}{3}\right)^2 = a'y^2 - \frac{2a'^2}{3}y + \frac{a'^3}{9},$$

$$b'x = b'\left(y - \frac{a'}{3}\right) = b'y - \frac{a'b'}{3}.$$

Adding all terms together with c', we get

$$x^3 + a'x^2 + b'x + c' = y^3 + \underbrace{\left(b' - \frac{a'^2}{3}\right)}_{p} y + \underbrace{\left(c' - \frac{a'b'}{3} + \frac{2a'^3}{27}\right)}_{q} = 0.$$

Thus, the cubic equation becomes

$$y^3 + py + q = 0,$$

with

$$p = b' - \frac{a'^2}{3}, \quad q = c' - \frac{a'b'}{3} + \frac{2a'^3}{27}.$$

5.a) En posant $y = u + v$, réécrire l'équation $y^3 + py + q = 0$ en fonction de u, v.

3pts

We start from the depressed cubic

$$y^3 + py + q = 0.$$

We make the substitution

$$y = u + v.$$

Then

$$y^3 = (u+v)^3 = u^3 + v^3 + 3uv(u+v).$$

Substituting into the equation gives

$$u^3 + v^3 + 3uv(u+v) + p(u+v) + q = 0.$$

Grouping terms, we have

$$u^3 + v^3 + (3uv + p)(u+v) + q = 0.$$

b) En imposant la condition $uv = -\frac{p}{3}$, donner une équation reliant u^3, v^3 et q.

3pts

Starting from

$$u^3 + v^3 + (3uv + p)(u+v) + q = 0,$$

we impose the condition

$$uv = -\frac{p}{3}.$$

Then

$$3uv + p = 3\left(-\frac{p}{3}\right) + p = -p + p = 0.$$

The equation simplifies to

$$u^3 + v^3 + q = 0.$$

6. Considérer l'équation quadratique (en z) $(z - u^3)(z - v^3) = 0$.
a) Réécrire l'équation avec des coefficients en fonction de p, q au lieu de u, v.

4pts

We consider the quadratic equation in z :

$$(z - u^3)(z - v^3) = 0.$$

Expanding, we get

$$z^2 - (u^3 + v^3)z + u^3v^3 = 0.$$

From the previous step, we know that

$$u^3 + v^3 = -q \quad \text{and} \quad uv = -\frac{p}{3}.$$

Therefore,

$$u^3v^3 = (uv)^3 = \left(-\frac{p}{3}\right)^3 = -\frac{p^3}{27}.$$

Substituting these expressions in terms of p and q, the quadratic equation becomes

$$z^2 + qz - \frac{p^3}{27} = 0.$$

b) À l'aide de votre formule dérivée en II-1, ou de toute autre technique, exprimer z en fonction de p et q.

4pts

The quadratic equation is

$$z^2 + qz - \frac{p^3}{27} = 0.$$

Using the quadratic formula, we get

$$z = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2}.$$

c) Sans perte de généralité, les deux solutions pour z doivent correspondre aux valeurs de u^3 et v^3. En déduire des expressions pour u et v.

2pts

From the previous step, we have the quadratic equation

$$z^2 + qz - \frac{p^3}{27} = 0,$$

with solutions

$$z = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2}.$$

Without loss of generality (WLOG), we can assign

$$u^3 = \frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2}, \quad v^3 = \frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2}.$$

Taking cube roots, we obtain

$$u = \sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2}}, \quad v = \sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2}}.$$

7. Finalement, donner une expression de y en fonction de q et p.

2pts

We have previously set

$$y = u + v,$$

with

$$u = \sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2}}, \quad v = \sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2}}.$$

Therefore, the solution for y in terms of p and q is

$$y = \sqrt[3]{\frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2}} + \sqrt[3]{\frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2}}$$

8. Désormais, on suppose que la formule pour $y^3 + py + q = 0$ est

$$y = \sqrt[3]{\frac{-q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{-q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Résoudre : $x^3 + 9x^2 + 33x + 25 = 0$.
Indication : après avoir trouvé une racine, factoriser puis utiliser la formule quadratique.

6pts

We start with the cubic equation

$$x^3 + 9x^2 + 33x + 25 = 0.$$

Step 1 : Depress the cubic. Let

$$x = y - \frac{a'}{3}, \quad a' = 9.$$

Then

$$x = y - 3.$$

Substitute into the cubic :

$$(y-3)^3 + 9(y-3)^2 + 33(y-3) + 25 = 0.$$

Expanding and simplifying, we get the depressed cubic

$$y^3 + 6y - 20 = 0.$$

Step 2 : Apply the formula.

$$y = \sqrt[3]{\frac{-q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{-q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

Substitute $p = 6$ and $q = -20$:

$$y = \sqrt[3]{10 - \sqrt{10^2 + 2^3}} + \sqrt[3]{10 + \sqrt{10^2 + 2^3}} = \sqrt[3]{10 - \sqrt{108}} + \sqrt[3]{10 + \sqrt{108}} = 2 \quad \textit{(Use calculator for the last step).}$$

Step 3 : Recover x from y.

$$x = y - 3 = -1.$$

Step 4 : Factorize by $x + 1$. We were given the cubic equation

$$x^3 + 9x^2 + 33x + 25 = 0.$$

$$x^3 + 9x^2 + 33x + 25 = (x+1)(x^2 + 8x + 25).$$

Step 5 : Solve the quadratic to find the two other roots.

$$x = \frac{-8 \pm \sqrt{8^2 - 4 \cdot 1 \cdot 25}}{2} = \frac{-8 \pm \sqrt{64 - 100}}{2} = \frac{-8 \pm \sqrt{-36}}{2} = \frac{-8 \pm 6i}{2} = -4 \pm 3i.$$

Finally, the three roots found are $x = -1, \quad x = -4 + 3i, \quad x = -4 - 3i$.

Nous avons trouvé une formule pour trouver une racine d'un polynôme de degré 1, 2 et 3.
Il existe une formule générale pour les polynômes de degré 4, mais elle ne tenait pas dans la marge de cette page...

II - Théorème fondamental de l'algèbre

Rappel : $z \in \mathbb{C}$ signifie $z = x + iy$ avec $x, y \in \mathbb{R}$, et $i = \sqrt{-1}$; de plus, $\Re(z) = a$, $\Im(z) = b$, $\overline{z} = x - iy$, et $|z| = \sqrt{x^2 + y^2}$.

0. a) Montrer que $\Re(z) \leq |z| = |\overline{z}| \quad \forall z \in \mathbb{C}$.

1pt

Since $y^2 \geq 0$, we have

$$x^2 \leq x^2 + y^2 \implies \Re(z) = x \leq |x| \leq \sqrt{x^2 + y^2} = |z|.$$

Moreover, for any complex number z, $\overline{z} = x - iy$ and

$$|\overline{z}| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|.$$

b) Montrer que $|z|^2 = z\overline{z} \quad \forall z \in \mathbb{C}$.

1pt

$|z| = \sqrt{x^2+y^2} \implies |z|^2 = x^2+y^2$.
$z\overline{z} = (x+iy)(x-iy) = x^2 - ixy + ixy - i^2y^2 = x^2+y^2$.

c) En calculant $|zw|^2$, montrer que $|zw| = |z||w| \quad \forall z, w \in \mathbb{C}$.

1pt

Using $|z|^2 = z\overline{z}$: $|zw|^2 = (zw)\overline{(zw)} = zw\,\overline{z}\,\overline{w} = (z\overline{z})(w\overline{w}) = |z|^2|w|^2$..
Since moduli are nonnegative, taking square roots gives $|zw| = |z|\,|w| \quad \forall z, w \in \mathbb{C}$.

d) En calculant $|z+w|^2$, montrer que $|z+w| \leq |z| + |w| \quad \forall z, w \in \mathbb{C}$ *(inégalité triangulaire)*.

4pts

It is trivial that $2\Re(\alpha) = \alpha + \overline{\alpha}$, applied to $w\overline{z}$, it yields $w\overline{z} + \overline{w\overline{z}} = w\overline{z} + z\overline{w} = 2\Re(z\overline{w})$.
We compute :

$$\begin{aligned} |z+w|^2 &= (z+w)\overline{(z+w)} \\ &= z\overline{z} + w\overline{z} + z\overline{w} + \overline{z}w \\ &= |z|^2 + |w|^2 + 2\Re(z\overline{w}) \\ &\leq |z|^2 + |w|^2 + 2|z||w| = (|z| + |w|)^2. \end{aligned}$$

Taking square roots gives $|z+w| \leq |z| + |w|$.

e) Justifier que $|z| - |w| \leq |z+w|$ (vous pouvez utiliser l'inégalité triangulaire ci-dessus).

2pts

By triangle inequality :

$$|z| = |(z+w) - w| \leq |z+w| + |w| \implies |z| - |w| \leq |z+w|.$$

L'objectif de cette section est de prouver que tout polynôme

$$p(z) = \sum_{k=0}^{n} a_k z^k \ , \quad a_k \in \mathbb{C}$$

a exactement n racines (disons z_k avec $k = 1, \ldots, n$).

1. a) Montrer que

$$\lim_{|z| \to +\infty} |p(z)| = +\infty.$$

4pts

Factor out the highest power of z :

$$p(z) = z^n \left(a_n + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_0}{z^n} \right).$$

Then the modulus is

$$|p(z)| = |z|^n \left| a_n + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_0}{z^n} \right|.$$

As $|z| \to +\infty$, the terms $\frac{a_{n-1}}{z}, \ldots, \frac{a_0}{z^n} \to 0$, so :

$$\left| a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_0}{z^n} \right| \to |a_n| > 0.$$

Therefore :

$$\lim_{|z| \to +\infty} |p(z)| = \lim_{|z| \to +\infty} |z|^n |a_n + o(1)| = +\infty.$$

b) En déduire qu'il existe R tel que : $|p(z)| > |p(0)| + 1, \quad \forall\ |z| > R$.

1pt

Direct definition of the previous result ($\lim_{|z|\to+\infty} |p(z)| = +\infty$).

c) En considérant $D = \{z \in \mathbb{C} \mid |z| \leq R\}$, montrer que $|p(z)|$ admet un minimum global.

2pts

Let $D = \{z \in \mathbb{C} \mid |z| \leq R\}$. Since D is compact and the function $z \mapsto |p(z)|$ is continuous, it attains a minimum on D (i.e. $\exists z_0 \in D$ s.t. $|p(z_0)| = \min_{z\in D} |p(z)|$).
Moreover, for $|z| > R$, we have $|p(z)| > |p(0)| + 1 \geq |p(z_0)|$, so z_0 is a global minimum of $|p(z)|$ on $\mathbb{C}$.
Les étudiants ne sont pas censés connaître la compacité, mais ils sont censés essayer de justifier cela « du mieux qu'ils peuvent » (avec un schéma, un argument écrit, ou toute chose pouvant convaincre la personne qui corrige qu'ils ont compris l'idée).

III - Lien avec la théorie des groupes

1. Considérons deux objets étiquetés 1 et 2. On appelle (1 2) la transformation (ou permutation) qui échange les deux objets, et (1) l'identité (aucun échange). L'exécution successive de deux transformations (deux permutations) sera notée $\star$.
De manière informelle, supposons que nous avons deux boules : une blanche (notée "W") et une noire (notée "B"). L'état initial est (W, B). Alors (1) est l'opération qui ne change pas l'état : $(1) \cdot (W, B) = (W, B)$, tandis que (1 2) est l'opération qui échange les deux objets : $(1\ 2) \cdot (W, B) = (B, W)$.
a) Calculer les compositions suivantes :

i) $(1\ 2) \star (1\ 2)$
ii) $(1) \star (1\ 2)$
iii) $(1\ 2) \star (1)$
iv) $(1) \star (1)$

2pts

i) $(1\ 2) \star (1\ 2) = (1)$; En effet, échanger deux fois remet chaque objet à sa place initiale.
ii) $(1) \star (1\ 2) = (1\ 2)$; La permutation identité laisse la permutation inchangée.
iii) $(1\ 2) \star (1) = (1\ 2)$; Composer avec l'identité laisse encore la permutation inchangée.
iv) $(1) \star (1) = (1)$; La composition de l'identité avec elle-même est l'identité.

b) Un ensemble S muni d'une opération $\cdot$ est appelé un *groupe* si les propriétés suivantes sont satisfaites :

— **Fermeture :** $\forall a, b \in S \quad a \cdot b \in S$
— **Associativité :** $\forall a, b, c \in S \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
— **Élément neutre :** $\exists\ e \in S$ tel que $\forall a \in S,\ a \cdot e = a = e \cdot a$
— **Inverse :** $\forall a \in S,\ \exists\ a^{-1} \in S$ tel que $a \cdot a^{-1} = e = a^{-1} \cdot a$

Montrer que l'ensemble $\{(1), (1\ 2)\}$, muni de l'opération $\star$, forme un groupe (appelé S_2).
Remarquez qu'ici, (1) et (1 2) sont des transformations ou fonctions (formellement appelées permutations), mais sont vues comme des éléments du groupe, i.e. $(1), (1\ 2) \in S_2$.

4pts

- Fermeture. D'après la partie (a), on a calculé :

$$(1) \star (1) = (1), \qquad (1) \star (1\ 2) = (1\ 2), \qquad (1\ 2) \star (1) = (1\ 2), \qquad (1\ 2) \star (1\ 2) = (1).$$

Dans chaque cas, le résultat appartient à S, donc S est stable par $\star$.
- Associativité. La composition de fonctions (donc de permutations) est associative, donc $\star$ est associative sur S.
- Élément neutre. La permutation (1) joue le rôle d'élément neutre pour la composition ($e = (1)$) :

$$(1) \star (1\ 2) = (1\ 2), \qquad (1\ 2) \star (1) = (1\ 2), \qquad \text{et } (1) \star (1) = (1).$$

- Inverses. Vérifions que tout élément de S admet un inverse dans S :

$$(1)^{-1} = (1) \quad \text{car} \quad (1) \star (1) = (1),$$

et

$$(1\ 2)^{-1} = (1\ 2) \quad \text{car} \quad (1\ 2) \star (1\ 2) = (1).$$

Ainsi, chaque élément possède un inverse dans S.

c) Un groupe est dit *abélien* si l'opération est commutative, c'est-à-dire si $\forall a, b \in S, \quad a \cdot b = b \cdot a$.
Le groupe S_2 est-il commutatif ? Justifier.

4pts

Pour le groupe $S_2 = \{(1), (1\ 2)\}$, vérifions tous les produits possibles :

$$(1) \star (1) = (1) = (1) \star (1), \quad (1) \star (1\ 2) = (1\ 2) = (1\ 2) \star (1), \quad (1\ 2) \star (1\ 2) = (1) = (1\ 2) \star (1\ 2).$$

Dans chaque cas, l'ordre de composition ne change pas le résultat, donc le groupe S_2 est commutatif (abélien).

d). Soit $x^2 + px + q = 0$ une équation du second degré de racines r_1 et r_2.

i) Écrire les racines r_1 et r_2 à l'aide de la formule quadratique.

2pts

D'après la formule du second degré :

$$r_1 = \frac{-p + \sqrt{p^2 - 4q}}{2}, \qquad r_2 = \frac{-p - \sqrt{p^2 - 4q}}{2}.$$

ii) Les deux racines peuvent être vues comme les objets déplacés par les permutations (1) et (1 2) (i.e. S_2). Donner une quantité impliquant r_1 et r_2 qui soit inchangée par cette permutation.

2pts

L'action de $S_2 = \{(1), (1\ 2)\}$ laisse la paire (r_1, r_2) inchangée ou bien échange les deux racines, i.e. :

$$(1)(r_1, r_2) = (r_1, r_2)$$
$$(1\ 2)(r_1, r_2) = (r_2, r_1)$$

Une quantité est inchangée par cet échange si elle est *symétrique* en r_1 et r_2. Par exemple, la somme $r_1 + r_2$ est invariante, car

$$(1\ 2) \cdot (r_1 + r_2) = r_2 + r_1 = r_1 + r_2.$$

(De façon équivalente, par les formules de Viète, $r_1 + r_2 = -p$, ce qui ne dépend pas de l'ordre des racines.)

2. Considérons maintenant trois objets étiquetés 1, 2 et 3. L'ensemble de toutes les permutations de $\{1, 2, 3\}$ muni de l'opération $\star$ (composition) est appelé S_3. On définit les permutations suivantes :

- On appelle (1) la permutation qui ne fait rien.
- On appelle (1 2) la permutation qui échange les objets 1 et 2.
- On appelle (1 3) la permutation qui échange les objets 1 et 3.
- On appelle (2 3) la permutation qui échange les objets 2 et 3.
- On appelle (1 2 3) la permutation qui effectue la rotation $1 \to 2$, $2 \to 3$ et $3 \to 1$.
- On appelle (1 3 2) la permutation qui effectue la rotation des objets 1, 2 et 3 dans l'autre sens ($1 \to 3$, $3 \to 2$ et $2 \to 1$).

a) Recopier et compléter le tableau suivant (appelé une *table de Cayley*) décrivant l'opération $\star$ sur S_3 :

$\star$	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)						
(1 2)						
(1 3)						
(2 3)						
(1 2 3)						
(1 3 2)						

6pts

$\star$	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	(1)	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	(1)	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	(1)	(1 2 3)

b) Le groupe S_3 est-il abélien ? Justifier.

2pts

Non, S_3 *n'est pas* abélien. Il suffit de trouver deux éléments qui ne commutent pas :

$$(1\ 2) \star (1\ 3) = (1\ 3\ 2), \qquad \text{mais} \qquad (1\ 3) \star (1\ 2) = (1\ 2\ 3).$$

Or

$$(1\ 3\ 2) \neq (1\ 2\ 3) \implies (1\ 2) \star (1\ 3) \neq (1\ 3) \star (1\ 2),$$

donc l'opération n'est pas commutative. Ainsi S_3 n'est pas abélien.

L'*ordre* de a, noté $\mathrm{ord}(a)$, est le plus petit entier positif n tel que $a^n = e$, où e est l'élément neutre. *(Si aucun entier positif n'existe, alors g est dit d'ordre infini.)*
c) Quel est l'ordre de (1 2 3) ? Quel est l'ordre de (2 3) ?

3pts

Ordre de (1 2 3)**.**

2pts

La permutation (1 2 3) fait cycler les éléments selon $1 \to 2$, $2 \to 3$, $3 \to 1$. Calculons ses puissances :

$$(1\ 2\ 3)^2 = (1\ 3\ 2), \qquad (1\ 2\ 3)^3 = (1).$$

Comme l'identité apparaît pour la première fois à la troisième puissance, on a $\mathrm{ord}(1\ 2\ 3) = 3$.
Ordre de (2 3)**.**

1pt

La permutation (2 3) est une transposition. En calculant son carré, on obtient $(2\ 3)^2 = (1)$. Ainsi, le plus petit entier positif n tel que $(2\ 3)^n = (1)$ est $n = 2$, donc $\mathrm{ord}(2\ 3) = 2$.

d) Un sous-ensemble non vide H d'un groupe G est appelé un *sous-groupe* s'il satisfait les propriétés suivantes :

- il contient l'élément neutre (i.e. $e \in H$) ;
- il est stable par l'opération du groupe (i.e. $\forall a, b \in H,\ a \cdot b \in H$) ;
- il est stable par passage à l'inverse (i.e. $\forall a \in H,\ a^{-1} \in H$).

Soit $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\} \subset S_3$.
Montrer que H est un sous-groupe de S_3.

3pts

- Élément neutre.
L'élément neutre de S_3 est (1), et clairement $(1) \in H$.
- Stabilité par $\star$.
Soient $a, b \in H$. On vérifie que $a \star b \in H$ en calculant les produits entre les trois éléments. En utilisant que (1) est l'identité et que

$$(1\ 2\ 3) \star (1\ 2\ 3) = (1\ 2\ 3)^2 = (1\ 3\ 2), \qquad (1\ 2\ 3) \star (1\ 3\ 2) = (1\ 2\ 3)^3 = (1),$$

et de même

$$(1\ 3\ 2) \star (1\ 3\ 2) = (1\ 3\ 2)^2 = (1\ 2\ 3), \qquad (1\ 3\ 2) \star (1\ 2\ 3) = (1),$$

on voit que tout produit de deux éléments de H est encore l'un de

$$(1),\ (1\ 2\ 3),\ (1\ 3\ 2),$$

donc appartient à H. Ainsi H est stable par $\star$.
- Stabilité par inverses.
On a

$$(1)^{-1} = (1) \in H.$$

De plus, comme $(1\ 2\ 3)^3 = (1)$, on obtient

$$(1\ 2\ 3)^{-1} = (1\ 2\ 3)^2 = (1\ 3\ 2) \in H,$$

et de même

$$(1\ 3\ 2)^{-1} = (1\ 3\ 2)^2 = (1\ 2\ 3) \in H.$$

Ainsi H est stable par inverses.

Comme H contient l'identité, est stable par l'opération $\star$ et est stable par passage à l'inverse, H est un sous-groupe de S_3.

3. Considérons maintenant cinq objets étiquetés $1, 2, 3, 4, 5$. L'ensemble de toutes les permutations de ces cinq objets muni de l'opération de composition $\star$ est appelé S_5. Un cycle $(a_1\ a_2\ \ldots\ a_k)$ envoie a_i sur a_{i+1} pour $i = 1, \ldots, k-1$, envoie a_k sur a_1, et fixe tous les autres éléments.
a) Combien y a-t-il de permutations différentes dans S_5 ? Ceci s'appelle la taille de S_5 et se note $|S_5|$.

2pts

Une permutation de l'ensemble $\{1, 2, 3, 4, 5\}$ est une bijection de cet ensemble vers lui-même. Pour construire une permutation, on peut choisir l'image de chaque élément :

- il y a 5 choix pour l'image de 1,
- une fois ceci choisi, il reste 4 choix pour l'image de 2,
- puis 3 choix pour l'image de 3,
- puis 2 choix pour l'image de 4,
- et enfin 1 choix pour l'image de 5.

En multipliant, le nombre total de permutations vaut $5 \times 4 \times 3 \times 2 \times 1 = 5!$. Ainsi $|S_5| = 5! = 120$.

b) Permutations simples.

i) Donner un exemple de permutation de S_5 d'ordre 2.
ii) Donner un exemple de permutation de S_5 d'ordre 3.
iii) Donner un exemple de permutation de S_5 d'ordre 5.
iv) Donner un exemple de permutation de S_5 d'ordre 6.

4pts

i) **Ordre 2.**
Toute transposition est d'ordre 2. Par exemple, $(1\ 2)$ vérifie $(1\ 2)^2 = (1)$, donc $\mathrm{ord}(1\ 2) = 2$.
ii) **Ordre 3.**
Tout 3-cycle est d'ordre 3. Par exemple, $(1\ 2\ 3)$ vérifie $(1\ 2\ 3)^3 = (1)$, donc $\mathrm{ord}(1\ 2\ 3) = 3$.
iii) **Ordre 5.**
Un 5-cycle est d'ordre 5. Par exemple, $(1\ 2\ 3\ 4\ 5)$ vérifie $(1\ 2\ 3\ 4\ 5)^5 = (1)$, donc $\mathrm{ord}(1\ 2\ 3\ 4\ 5) = 5$.
iv) **Ordre 6.** ***Remarque :*** *Pour une permutation écrite comme produit de cycles* disjoints*, son ordre est le ppcm des longueurs de ces cycles.*
Considérons un produit de cycles disjoints de longueurs 3 et 2, par exemple $(1\ 2\ 3)(4\ 5)$. L'ordre vaut $\mathrm{lcm}(3, 2) = 6$, donc cette permutation est d'ordre 6.

c) Le groupe S_5 est-il abélien ? Justifier.

2pts

Non, S_5 *n'est pas* abélien.
Pour le justifier, il suffit de trouver deux permutations de S_5 qui ne commutent pas :
Soient $\sigma = (1\ 2)$ et $\tau = (2\ 3)$. Calculons les compositions :

$$\sigma \star \tau = (1\ 2) \star (2\ 3) = (1\ 2\ 3), \quad \text{tandis que} \quad \tau \star \sigma = (2\ 3) \star (1\ 2) = (1\ 3\ 2).$$

Comme $(1\ 2\ 3) \neq (1\ 3\ 2)$, on a $\sigma \star \tau \neq \tau \star \sigma$. Donc l'opération n'est pas commutative, et S_5 n'est pas abélien.

d) Une *transposition* est une permutation qui échange exactement deux objets et laisse tous les autres inchangés.

i) Écrire le cycle (1 2 3) comme produit de deux transpositions.

1pt

On affirme que $(1\ 2\ 3) = (1\ 3)(1\ 2)$. En effet, en appliquant d'abord le membre de droite :

$$1 \xrightarrow{(1\ 2)} 2 \xrightarrow{(1\ 3)} 2, \quad 2 \xrightarrow{(1\ 2)} 1 \xrightarrow{(1\ 3)} 3, \quad 3 \xrightarrow{(1\ 2)} 3 \xrightarrow{(1\ 3)} 1,$$

donc au total $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, ce qui est exactement $(1\ 2\ 3)$.

ii) Écrire le cycle (1 2 3 4) comme produit de transpositions (ce cycle envoie $1 \to 2$, $2 \to 3$, $3 \to 4$ et $4 \to 1$).

2pts

On affirme que $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$. En effet, en appliquant d'abord le membre de droite :

$$1 \xrightarrow{(1\ 2)} 2 \xrightarrow{(1\ 3)} 2 \xrightarrow{(1\ 4)} 2, \quad 2 \xrightarrow{(1\ 2)} 1 \xrightarrow{(1\ 3)} 3 \xrightarrow{(1\ 4)} 3, \quad 3 \xrightarrow{(1\ 2)} 3 \xrightarrow{(1\ 3)} 1 \xrightarrow{(1\ 4)} 4, \quad 4 \xrightarrow{(1\ 2)} 4 \xrightarrow{(1\ 3)} 4 \xrightarrow{(1\ 4)} 1,$$

donc au total $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$ et $4 \mapsto 1$, ce qui est exactement $(1\ 2\ 3\ 4)$.

iii) Montrer qu'un cycle général $(1\ 2\ \ldots\ k)$ peut s'écrire comme produit de transpositions de la forme $(a_1\ a_i)$ (ce cycle envoie $1 \to 2$, $2 \to 3$, …, $(k-1) \to k$, $k \to 1$).

3pts

Nous allons montrer que pour $k \geq 2$, on a

$$(1\ 2\ \ldots\ k) = (1\ k)(1\ k-1)\cdots(1\ 3)(1\ 2).$$

Posons $\sigma = (1\ k)(1\ k-1)\cdots(1\ 2)$. Calculons $\sigma(i)$:

- Pour $i = 1$: la transposition la plus à droite $(1\ 2)$ envoie $1 \mapsto 2$, et aucune des transpositions restantes ne déplace 2, donc $\sigma(1) = 2$.
- Plus généralement, pour $1 \leq i \leq k-1$: la transposition $(1\ i)$ envoie $i \mapsto 1$, puis la transposition suivante à gauche, $(1\ i+1)$, envoie $1 \mapsto i+1$. Aucune autre transposition n'affecte $i+1$, donc $\sigma(i) = i+1$.
- Pour $i = k$: la transposition $(1\ k)$ envoie $k \mapsto 1$, et aucune transposition à gauche ne change ensuite 1, donc $\sigma(k) = 1$.
- Tout élément hors de $\{1, 2, \ldots, k\}$ est fixé par chaque transposition, donc est fixé par σ.

Ainsi σ agit comme $1 \mapsto 2 \mapsto \cdots \mapsto k \mapsto 1$, donc $\sigma = (1\ 2\ \ldots\ k)$.

iv) Montrer qu'une permutation générale peut s'écrire comme produit de transpositions.

4pts

En renommant l'argument de (iii), on obtient la décomposition standard

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_3)(a_1\ a_2),$$

qui est un produit de transpositions.
Soit $\sigma \in S_n$ une permutation quelconque. Nous allons partitionner $\{1, 2, \ldots, n\}$ en cycles déterminés par l'action de σ. Choisissons un élément a_1. Considérons son orbite sous σ :

$$a_1,\ \sigma(a_1),\ \sigma^2(a_1),\ \ldots$$

Comme l'ensemble est fini, il existe des entiers $i < j$ tels que $\sigma^i(a_1) = \sigma^j(a_1)$. En appliquant σ^{-i}, on obtient $a_1 = \sigma^{j-i}(a_1)$. Soit k le plus petit entier strictement positif tel que $\sigma^k(a_1) = a_1$. Alors les

éléments $a_1,\ a_2 = \sigma(a_1),\ a_3 = \sigma^2(a_1),\ \ldots,\ a_k = \sigma^{k-1}(a_1)$ sont tous distincts, et sur cet ensemble σ agit par $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, donc σ se restreint au cycle $(a_1\ a_2\ \cdots\ a_k)$.
Si ce cycle n'inclut pas tous les éléments de $\{1, \ldots, n\}$, choisissons b_1 n'appartenant pas à $\{a_1, \ldots, a_k\}$ et répétons la même construction pour obtenir un autre cycle. En continuant, on épuise tous les éléments. Les cycles obtenus sont disjoints car ils proviennent d'orbites disjointes, et sur chaque orbite σ coïncide avec le cycle correspondant, tout en fixant les éléments hors de cette orbite. Ainsi σ est égale au produit de ces cycles disjoints.
Comme chaque cycle est un produit de transpositions par la formule ci-dessus, on en déduit que toute permutation est un produit de transpositions.

4. Rappelons que S_5 est le groupe de toutes les permutations de cinq objets. Une permutation est dite *paire* si elle peut s'écrire comme produit d'un nombre pair de transpositions. L'ensemble de toutes les permutations paires de S_5 est appelé le *groupe alterné* A_5.
a) Montrer que A_5 est un sous-groupe de S_5.

4pts

- Identité.
La permutation identité (1) peut s'écrire comme produit de 0 transposition, et 0 est pair. Donc $(1) \in A_5$.
- Stabilité par composition.
Soient $\sigma, \tau \in A_5$. Alors il existe des transpositions $t_1, \ldots, t_{2m}$ et $s_1, \ldots, s_{2n}$ telles que

$$\sigma = t_1 t_2 \cdots t_{2m}, \qquad \tau = s_1 s_2 \cdots s_{2n}.$$

Alors

$$\sigma \star \tau = \sigma\tau = (t_1 t_2 \cdots t_{2m})(s_1 s_2 \cdots s_{2n}),$$

qui est un produit de $2m + 2n$ transpositions. Comme $2m + 2n$ est pair, on a $\sigma \star \tau \in A_5$.
- Stabilité par inverses.
Soit $\sigma \in A_5$ avec $\sigma = t_1 t_2 \cdots t_{2m}$ un produit de $2m$ transpositions. En inversant et en utilisant $(ab)^{-1} = b^{-1}a^{-1}$, on obtient

$$\sigma^{-1} = (t_1 t_2 \cdots t_{2m})^{-1} = t_{2m}^{-1} \cdots t_2^{-1} t_1^{-1}.$$

Or chaque transposition est son propre inverse, $t_i^{-1} = t_i$, donc

$$\sigma^{-1} = t_{2m} \cdots t_2 t_1,$$

qui est encore un produit de $2m$ transpositions, donc d'un nombre pair. Ainsi $\sigma^{-1} \in A_5$.

Comme A_5 contient l'identité, est stable par l'opération du groupe, et est stable par passage à l'inverse, c'est un sous-groupe de S_5.

b) Montrer qu'exactement la moitié des permutations de S_5 sont paires. En déduire la taille de $|A_5|$.

4pts

Soit $\tau = (1\ 2)$ une transposition ; définissons l'application

$$f : S_5 \to S_5, \qquad f(\sigma) = \tau \star \sigma = \tau\sigma.$$

Affirmation 1 : f est une bijection.
En effet, f est sa propre réciproque, puisque $\tau^{-1} = \tau$:

$$f(f(\sigma)) = \tau(\tau\sigma) = (\tau^2)\sigma = (1)\sigma = \sigma.$$

Donc f est une bijection.
Affirmation 2 : f échange la parité (pair $\leftrightarrow$ impair).
Si σ est paire, écrivons σ comme produit de $2m$ transpositions. Alors $f(\sigma) = \tau\sigma$ est un produit de $2m+1$ transpositions, donc est impaire. Réciproquement, si σ est impaire (produit de $2m + 1$ transpositions), alors $\tau\sigma$ est un produit de $2m + 2$ transpositions, donc est paire.
Ainsi f fournit une bijection entre l'ensemble des permutations paires et celui des permutations impaires. Par conséquent, le nombre de permutations paires est égal au nombre de permutations impaires, donc *exactement la moitié* des éléments de S_5 sont paires.

Comme $|S_5| = 5! = 120$, on conclut que

$$|A_5| = \frac{|S_5|}{2} = 60.$$

5. Soit G un groupe. Deux éléments $g, h \in G$ sont dits dans la même classe s'il existe un élément $x \in G$ tel que $h = xgx^{-1}$. L'ensemble de tous les éléments reliés à g de cette façon s'appelle la *classe* de g.
a) Montrer que l'élément neutre forme à lui seul une classe.

1pts

Pour tout $x \in G$, on a $xex^{-1} = e$, donc le conjugué de e est toujours e. Ainsi la classe de e est $\{xex^{-1} : x \in G\} = \{e\}$ (i.e. elle ne contient que l'identité).

b) Expliquer pourquoi un élément ne peut pas appartenir simultanément à deux classes différentes.

4pts

Définissons une relation $\sim$:

$$g \sim h \quad \Longleftrightarrow \quad \exists x \in G \text{ tel que } h = xgx^{-1}.$$

C'est la relation usuelle de *conjugaison*, et c'est une relation d'équivalence :

- Réflexive : $g = ege^{-1}$, donc $g \sim g$.
- Symétrique : si $h = xgx^{-1}$ alors $g = x^{-1}hx$, donc $h \sim g$.
- Transitive : si $h = xgx^{-1}$ et $k = yhy^{-1}$ alors $k = y(xgx^{-1})y^{-1} = (yx)g(yx)^{-1}$, donc $g \sim k$.

Ainsi les classes sont exactement les classes d'équivalence de $\sim$, et deux classes d'équivalence sont soit identiques soit disjointes. Donc un élément ne peut pas appartenir à deux classes différentes à la fois.

c) Comparer $|G|$ avec la somme des tailles de toutes les classes.

2pts

Comme les classes de conjugaison sont disjointes et que leur réunion vaut G, elles forment une partition de G.
Ainsi,

$$|G| = \sum_{\mathcal{C} \subseteq G} |\mathcal{C}|,$$

où la somme porte sur toutes les classes de conjugaison $\mathcal{C}$ de G.

6. Un sous-groupe H d'un groupe G est dit *invariant* (ou *normal*) si pour tout $g \in G$ et tout $h \in H$, l'élément ghg^{-1} appartient encore à H. Dans ce cas, on note $H \triangleleft G$.

a) Soit H un sous-groupe invariant de G et soit $h \in H$. Expliquer pourquoi la classe entière de h doit être contenue dans H.

4pts

Supposons $H \triangleleft G$. Soit $h \in H$ et soit $x \in G$ arbitraire. Alors, par la définition d'un sous-groupe invariant, on a $xhx^{-1} \in H$. Ainsi tout conjugué de h par un élément de G appartient à H. Autrement dit, la classe de conjugaison de h dans G est contenue dans H.

b) En conclure que tout sous-groupe invariant est une réunion de classes entières, en plus de l'identité.

2pt

Cela découle directement de (a) et du fait que l'élément neutre doit appartenir à H (puisque H est un sous-groupe).

7. Nous allons démontrer le **théorème de Lagrange** : l'ordre de tout sous-groupe divise l'ordre du groupe.
Supposons que G est un groupe fini et que H est un sous-groupe de G.

a) Soit $g \in G$, définir l'ensemble $gH = \{gh \mid h \in H\}$. Expliquer pourquoi $gH \subseteq G$.

1pt

Comme $g \in G$ et $H \subseteq G$, pour tout $h \in H$ on a $h \in G$. Comme G est un groupe, il est stable par l'opération, donc le produit gh appartient à G. Ainsi tout élément de la forme gh appartient à G, ce qui montre que $gH \subseteq G$.

b) Montrer que si $g_1H = g_2H$, alors $g_2^{-1}g_1 \in H$. Réciproquement, montrer que si $g_2^{-1}g_1 \in H$, alors $g_1H = g_2H$.

2pts

Supposons d'abord que $g_1H = g_2H$. Comme $g_1 \in g_1H$, on a $g_1 \in g_2H$, donc il existe $h \in H$ tel que $g_1 = g_2h$. En multipliant à gauche par g_2^{-1}, on obtient $g_2^{-1}g_1 = h \in H$.
Réciproquement, supposons que $g_2^{-1}g_1 \in H$. Alors il existe $h \in H$ tel que $g_2^{-1}g_1 = h$, donc $g_1 = g_2h$. Pour tout $h' \in H$, on a $g_1h' = g_2(hh') \in g_2H$, puisque H est un sous-groupe et donc stable par produit. Ainsi $g_1H \subseteq g_2H$. Par symétrie, l'inclusion réciproque est vraie, donc $g_1H = g_2H$.

c) En déduire que pour tous $g_1, g_2 \in G$, les ensembles g_1H et g_2H sont soit égaux soit disjoints.

2pts

Si $g_1H = g_2H$, c'est terminé. Sinon, supposons que $g_1H \cap g_2H \neq \varnothing$. Alors il existe $x \in G$ tel que $x = g_1h_1 = g_2h_2$ pour certains $h_1, h_2 \in H$. On réécrit : $g_2^{-1}g_1 = h_2h_1^{-1} \in H$, puisque H est un sous-groupe. Par le résultat précédent, cela implique $g_1H = g_2H$. Donc, si $g_1H \neq g_2H$, l'intersection est vide, et les deux ensembles sont disjoints.

d) Définir la fonction $f : H \to gH \quad \text{par} \quad f(h) = gh$. Montrer que f est une bijection.

2pts

Montrons d'abord que f est injective. Supposons $f(h_1) = f(h_2)$ pour certains $h_1, h_2 \in H$. Alors $gh_1 = gh_2$, et en multipliant à gauche par g^{-1} on obtient $h_1 = h_2$. Donc f est injective.
Montrons ensuite que f est surjective. Par définition de gH, tout élément $x \in gH$ s'écrit $x = gh$ pour un certain $h \in H$. Alors $x = f(h)$, donc tout élément de gH est dans l'image de f. Ainsi f est surjective.
Comme f est à la fois injective et surjective, c'est une bijection.

e) En déduire que tout ensemble de la forme gH contient exactement $|H|$ éléments.

2pts

D'après la question précédente, l'application $f : H \to gH$ définie par $f(h) = gh$ est une bijection. Une bijection met en correspondance chaque élément de H avec exactement un élément de gH, et réciproquement. Donc H et gH ont le même nombre d'éléments, d'où $|gH| = |H|$.

f) Expliquer pourquoi G peut s'écrire comme réunion disjointe de k ensembles distincts de la forme gH, chacun contenant exactement $|H|$ éléments, pour un certain entier k.

2pts

Tout élément $g \in G$ appartient à la classe à gauche gH (car $g = g \cdot e$ et $e \in H$), donc l'union de tous les ensembles de la forme gH est égale à G. D'après le résultat précédent, deux classes g_1H et g_2H sont soit égales soit disjointes, donc les classes distinctes forment une partition de G. Comme G est fini, il n'y a qu'un nombre fini de classes distinctes ; notons-le k. Chaque classe contient $|H|$ éléments, donc G est une réunion disjointe de k classes à gauche distinctes, chacune de taille $|H|$.

g) Conclure que $|H|$ divise $|G|$.

1pt

Comme G est la réunion disjointe de k classes à gauche distinctes de H, et que chaque classe contient exactement $|H|$ éléments, on a

$$|G| = k\,|H|$$

pour un certain entier k. Donc $|H|$ divise $|G|$.

Un groupe sans sous-groupe invariant propre (aucun autre sous-groupe invariant que lui-même et $\{e\}$) est dit *simple*.
f) Les tailles des classes de A_5 sont $1, 12, 12, 20, 15$. Conclure que A_5 est simple.

4pts

Soit $H \trianglelefteq A_5$ avec $e \in H$. Comme H est invariant, il doit être une réunion de classes de conjugaison, donc sa taille est

$$|H| = 1 + (\text{une somme de } 12, 12, 20, 15).$$

Les valeurs possibles sont donc :

$$\begin{aligned}
&1,\\
&1+12=13, \quad 1+20=21, \quad 1+15=16,\\
&1+12+12=25, \quad 1+12+20=33, \quad 1+12+15=28,\\
&1+12+20=33, \quad 1+12+15=28, \quad 1+20+15=36,\\
&1+12+12+20=45, \quad 1+12+12+15=40, \quad 1+12+20+15=48,\\
&1+12+12+20+15=60.
\end{aligned}$$

Comme H est un sous-groupe, sa taille $|H|$ doit diviser $|A_5| = 60$. Par conséquent, les seules tailles possibles sont $|H| = 1$ et $|H| = 60$.

8. Un groupe G est dit *résoluble* si sa *série dérivée* atteint finalement le sous-groupe trivial :

$$G^{(0)} = G, \qquad G^{(1)} = [G, G], \qquad G^{(2)} = [G^{(1)}, G^{(1)}], \ \ldots$$

où $[G, G]$ est le sous-groupe engendré par tous les *commutateurs* $[g, h] = ghg^{-1}h^{-1} \quad (g, h \in G)$, c'est-à-dire :

$$[G, G] = \langle\, [g, h] \mid g, h \in G \rangle.$$

G est résoluble s'il existe un entier n tel que $G^{(n)} = \{e\}$.
Le but de cette question est de montrer que S_5 n'est pas résoluble.

a) Montrer que pour tout groupe G, le sous-groupe des commutateurs $[G, G]$ est un sous-groupe *normal* de G.

3pts

Rappelons que $[G, G]$ est engendré par tous les commutateurs $[a, b] = aba^{-1}b^{-1}$ avec $a, b \in G$. Soit $g \in G$ et soit $[a, b]$ un commutateur. Alors

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1},\, gbg^{-1}],$$

qui est encore un commutateur d'éléments de G. Ainsi $g[a, b]g^{-1} \in [G, G]$. Comme la conjugaison préserve les produits, le conjugué de tout produit de commutateurs appartient encore à $[G, G]$. Donc $[G, G]$ est normal dans G.

Le groupe quotient $G/[G, G]$ est l'ensemble des classes à gauche du sous-groupe des commutateurs $[G, G]$ dans G :

$$G/[G, G] = \{\, g[G, G] \mid g \in G \,\}.$$

L'opération de groupe est définie par

$$(g[G, G])\,(h[G, G]) = (gh)[G, G],$$

pour tous $g, h \in G$. Cette opération est bien définie car $[G, G]$ est un sous-groupe normal de G.
b) Montrer que le groupe quotient $G/[G, G]$ est abélien.

4pts

Soient $g, h \in G$ et considérons leurs classes dans $G/[G, G]$. On a

$$(g[G, G])(h[G, G]) = (gh)[G, G] \quad \text{et} \quad (h[G, G])(g[G, G]) = (hg)[G, G].$$

Or

$$gh = (ghg^{-1}h^{-1})\, hg = [g, h]\, hg.$$

Comme $[g, h] \in [G, G]$, on voit que gh et hg diffèrent par la multiplication par un élément de $[G, G]$. Par définition des classes, deux éléments appartiennent à la même classe modulo $[G, G]$ si et seulement si leur produit diffère d'un élément de $[G, G]$. Ainsi

$$(gh)[G, G] = ([g, h]\, hg)[G, G] = (hg)[G, G],$$

puisque multiplier par un élément de $[G,G]$ ne change pas la classe.
Donc

$$(g[G,G])(h[G,G]) = (h[G,G])(g[G,G])$$

pour toutes les classes, et $G/[G,G]$ est abélien.

c) En déduire que si G n'est *pas* abélien, alors $[G,G] \neq \{e\}$.

2pts

Supposons par l'absurde que $[G,G] = \{e\}$. Alors le groupe quotient $G/[G,G]$ n'est autre que $G/\{e\} \cong G$. Mais on a montré que $G/[G,G]$ est abélien, donc G serait abélien, contradiction. Ainsi, si G n'est pas abélien, alors $[G,G] \neq \{e\}$.

d) À l'aide des parties précédentes, en déduire que $A_5^{(1)} = [A_5, A_5]$ est un sous-groupe *normal non trivial* de A_5.

1pt

Comme A_5 n'est pas abélien (partie précédente), on a $[A_5, A_5] \neq \{e\}$. De plus, pour tout groupe G, le sous-groupe des commutateurs $[G,G]$ est normal dans G (partie précédente), donc $[A_5, A_5] \trianglelefteq A_5$. Ainsi $A_5^{(1)} = [A_5, A_5]$ est un sous-groupe normal non trivial de A_5.

e) Conclure que $[A_5, A_5] = A_5$.

1pt

D'après le résultat précédent, $[A_5, A_5]$ est un sous-groupe normal non trivial de A_5. Or A_5 n'a pas de sous-groupe normal non trivial propre, donc la seule possibilité est $[A_5, A_5] = A_5$.

f) Conclure que A_5 n'est pas résoluble.

1pt

On a montré que $A_5^{(1)} = [A_5, A_5] = A_5$. Donc $A_5^{(2)} = [A_5^{(1)}, A_5^{(1)}] = [A_5, A_5] = A_5$, et par récurrence $A_5^{(n)} = A_5$ pour tout $n \geq 1$. La série dérivée n'atteint donc jamais $\{e\}$: il n'existe pas de n tel que $A_5^{(n)} = \{e\}$. Ainsi A_5 n'est pas résoluble.

g) Montrer par récurrence sur n que si G est résoluble et si $H \leq G$, alors la série dérivée vérifie $H^{(n)} \leq G^{(n)}$ pour tout n.

3pts

Pour $n = 0$, on a $H^{(0)} = H \leq G = G^{(0)}$.

Supposons $H^{(n)} \leq G^{(n)}$ pour un certain $n \geq 0$.
Alors tout commutateur d'éléments de $H^{(n)}$ est aussi un commutateur d'éléments de $G^{(n)}$. Donc le sous-groupe engendré par ces commutateurs vérifie

$$H^{(n+1)} = [H^{(n)}, H^{(n)}] \ \leq \ [G^{(n)}, G^{(n)}] = G^{(n+1)}.$$

Ainsi l'assertion est vraie au rang $n+1$.
Par récurrence, $H^{(n)} \leq G^{(n)}$ pour tout $n \geq 0$.

h) Conclure que S_5 n'est pas résoluble.

2pts

Supposons par l'absurde que S_5 soit résoluble. Comme $A_5 \leq S_5$, le résultat précédent implique $A_5^{(n)} \leq S_5^{(n)}$ pour tout n. Puisque S_5 est résoluble, il existe n tel que $S_5^{(n)} = \{e\}$, donc $A_5^{(n)} = \{e\}$ aussi. Cela signifierait que A_5 est résoluble, contradiction avec le fait que A_5 n'est pas résoluble. Donc S_5 n'est pas résoluble.

*On peut montrer qu'un polynôme $f(x)$ est **résoluble par radicaux** (c'est-à-dire que ses racines peuvent s'exprimer à l'aide d'un nombre fini d'opérations arithmétiques et de radicaux) si et seulement si le groupe de symétrie de ses racines—appelé son **groupe de Galois** $G = \mathrm{Gal}(f/K)$—est un **groupe résoluble**.*
Dans cet examen, vous avez démontré que le groupe symétrique S_5 n'est pas résoluble. Pour un polynôme général de degré 5, le groupe de symétrie de ses racines est S_5. Il ne peut donc pas exister de formule générale (par radicaux) pour les racines d'un polynôme de degré 5.
Plus généralement, on peut montrer que les groupes symétriques S_n ne sont pas résolubles pour tout $n \geq 5$. Cela implique qu'il n'existe pas de formule générale par radicaux pour les racines d'un polynôme de degré strictement supérieur à quatre.
Ceci explique pourquoi il existe des formules explicites pour les équations du second, troisième et quatrième degré, mais pas pour celles de degré cinq ou plus.

IV - À la gloire de Galois

1. Dériver une formule générale pour résoudre les équations quintiques par radicaux. Bonne chance.

1000pts