L'EVARISTE

Morning Exam

Durée : 2 heures

ALBERTSCHOOL D E Shaw & Co

Each section has question with increasing difficulty. It is allowed to skip some questions if you are blocked.

I - Warming up

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

1pt

The solution to the equation is $x = -\frac{b}{a}$.

b) Use your formula to solve $5x + 7 = 0$.

1pt

The solution to the equation is $x = -\frac{7}{5}$.

2. a) By completing the square, solve $ax^2 + bx + c = 0$ $(a, b, c \in \mathbb{R},\ a \neq 0)$.

8pts

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

b) Use your formula, or any other method to solve the following equations :

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

2pts

$x = -3$ or $x = 2$

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

2pts

$x = 11$ or $x = 13$

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

2pts

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

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

2pts

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

3. We will now consider the equation $ax^3 + bx^2 + cx + d = 0$ $(a, b, c, d \in \mathbb{R},\ a \neq 0)$. Justify that this equation can be rescaled to $x^3 + a'x^2 + b'x + c' = 0$.

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. Using $x = y - \frac{a'}{3}$, show that the above equation is equivalent to $y^3 + py + q = 0$, expressing p and q in terms of 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) Letting $y = u + v$, rewrite the equation $y^3 + py + q = 0$ in terms of 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) Imposing the condition $uv = -\frac{p}{3}$, give an equation linking u^3, v^3 and 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. Consider the quadratic (in z) equation $(z - u^3)(z - v^3) = 0$.
a) Rewrite the equation with the coefficients in terms of p, q instead of 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) Using your formula derived in II-1, or any other technique, express z in terms of p and 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) WLOG, the two solutions for z must correspond to the value of u^3 and v^3. Deduct expressions for u and 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. Finally, give an expression for y in terms of q and 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. From now on, it is assumed that the formula for $y^3 + py + q = 0$ is

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

Solve : $x^3 + 9x^2 + 33x + 25 = 0$.
Hint : after finding one root, factorize and use quadratic formula.

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 $x = -1, \quad x = -4 + 3i, \quad x = -4 - 3i$.

We have found a formula to find a root for a polynomial of degree 1, 2 and 3.
There exists a general formula for degree 4 polynomials, but it did not fit in the margin of this page...

II - Fundamental Theorem of Algebra

Reminder : $z \in \mathbb{C}$ means $z = x + iy$ with $x, y \in \mathbb{R}$, and $i = \sqrt{-1}$; moreover, $\Re(z) = a$, $\Im(z) = b$, $\overline{z} = x - iy$, and $|z| = \sqrt{x^2 + y^2}$.

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

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) Show that $|z|^2 = z\overline{z} \quad \forall z \in \mathbb{C}$.

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) By computing $|zw|^2$, show that $|zw| = |z||w| \quad \forall z, w \in \mathbb{C}$.

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) By computing $|z+w|^2$, show that $|z+w| \leq |z| + |w| \quad \forall z, w \in \mathbb{C}$ *(this is called triangle inequality).*

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) Justify that $|z| - |w| \leq |z+w|$ (you may use triangle inequality as stated above).

2pts

By triangle inequality :

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

The goal of this section is to prove that any polynomial

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

has n roots (say z_k with $k = 1, \ldots, n$).

1. a) Show that

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

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) Deduce that there exists R such that : $|p(z)| > |p(0)| + 1, \quad \forall\, |z| > R$.

1pt

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

c) Considering $D = \{z \in \mathbb{C} \mid |z| \leq R\}$, show that $|p(z)|$ has a global minimum.

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 $\mathbb{C}$.
Students are not meant to know about compactness, but they are meant to try to justify this "the best way they can" (with a diagram, a written argument, or anything that can make the person marking think that they understood what is going on.

2. Let this global minimum of $|p(z)|$ be z_0. This means that $\forall z \in \mathbb{C},\ |p(z_0)| \leq |p(z)|$.
We now assume (for contradiction) that $|p(z_0)| > 0$.
We will show that $\exists\ w \neq 0$ s.t. $|p(z_0 + w)| < |p(z_0)|$.

Let $w = z - z_0$ and $P(w) = p(z_0 + w)$ (p and P both have degree n). Denote $b_k \in \mathbb{C}$ the coefficients of P :

$$P(w) = \sum_{k=0}^{n} b_k w^k.$$

a) Express b_0 using p.

1pt

The constant term of P corresponds to $w = 0$: $b_0 = P(0) = p(z_0 + 0) = p(z_0)$

We rewrite [1]

$$P(w) = b_0 + w^{k_0}\left(\sum_{k=k_0}^{n} b_k w^{k-k_0}\right) \quad \text{with } b_k = 0 \quad \forall\ 0 < k < k_0.$$

Furthermore, let

$$q(w) = \sum_{k=k_0}^{n} b_k w^{k-k_0},$$

and note that $q(0) = b_{k_0} \neq 0$.

b) Express $p(z)$ in terms of $z - z_0$, $q(z - z_0)$, $p(z_0)$ (and k_0).

1pt

$$P(w) = p(z_0 + w) = b_0 + w^{k_0} q(w), \quad \text{with } b_0 = p(z_0) \text{ and } q(0) = b_{k_0} \neq 0$$

Substituting $w = z - z_0$, we get :

$$p(z) = p(z_0) + (z - z_0)^{k_0} q(z - z_0).$$

3. In this question, we make the approximation $w^{k_0} q(w) \approx w^{k_0} q(0)$. This is justified because q is continuous, and $|w|$ is small (w is close to 0). The next question will focus on making this argument rigorous.

Our goal is to make $|p(z_0 + w)|$ smaller than $|p(z_0)|$ by choosing w so that $p(z_0)$ and $w^{k_0} q(0)$ "point in opposite direction".

We use polar coordinates :

$$p(z_0) = Re^{i\alpha}, \quad R > 0$$
$$q(0) = Se^{i\beta}, \quad S > 0$$
$$w = re^{i\theta}, \quad r > 0$$

a) Give expressions in terms of r,S,β,θ for w^{k_0} and $w^{k_0} q(0)$.

1. It is possible that there is no $b_k = 0$, in which case, $k_0 = 1$.

1pt

$$w^{k_0} = (re^{i\theta})^{k_0} = r^{k_0} e^{ik_0\theta}$$
$$w^{k_0} q(0) = r^{k_0} e^{ik_0\theta} \cdot Se^{i\beta} = r^{k_0} S\, e^{i(k_0\theta+\beta)}$$

b) Find θ such that $\arg(w^{k_0} q(0)) \equiv \arg(p(z_0)) + \pi \mod 2\pi$.

3pts

We have
$$\arg(w^{k_0} q(0)) = k_0\theta + \beta$$
and
$$\arg(p(z_0)) = \alpha.$$
So we want
$$k_0\theta + \beta \equiv \alpha + \pi \pmod{2\pi}.$$
So solving for θ gives :
$$\theta = \frac{\alpha - \beta + \pi}{k_0} \pmod{\frac{2\pi}{k_0}}$$

c) With such θ, compute $w^{k_0} q(0)$ in terms of r, S, α, and k.

2pts

With $\theta = \frac{\alpha-\beta+\pi}{k_0}$, we have $w^{k_0} q(0) = r^{k_0} S\, e^{i(k_0\theta+\beta)} = r^{k_0} S\, e^{i(\alpha+\pi)} = -r^{k_0} S\, e^{i\alpha}$.

d) Therefore, show that $|p(z_0) + w^{k_0} q(0)| < R$.

2pts

We have $p(z_0) + w^{k_0} q(0) \approx Re^{i\alpha} + \left(-r^{k_0} Se^{i\alpha}\right) = (R - r^{k_0} S)e^{i\alpha}$.
Taking modulus : $|p(z_0) + w^{k_0} q(0)| \approx R - r^{k_0} S < R$.

e) Derive a contradiction, under the assumption that $w^{k_0} q(w) \approx w^{k_0} q(0)$.

2pts

Assuming $w^{k_0} q(w) \approx w^{k_0} q(0)$, we have :
$$|p(z)| = |p(z_0 + w)| \approx |p(z_0) + w^{k_0} q(0)| < R = |p(z_0)|.$$
This contradicts the definition of z_0 as a global minimum of $|p(z)|$.

4. Extract the "error term" of the approximation made above : let
$$E(w) = w^{k_0}(q(w) - q(0))$$

a) Express $P(w)$ in terms of b_0, $w^{k_0} q(0)$, and $E(w)$.

2pts

By definition,
$$P(w) = b_0 + w^{k_0} q(w) = b_0 + w^{k_0} q(0) + E(w).$$

b) Argue that $\lim_{w\to 0} q(w) = q(0)$.

2pts

The function $q(w) = \sum_{k=k_0}^{n} b_k w^{k-k_0}$ is a polynomial in w, hence continuous.
Therefore, by continuity at 0 :
$$\lim_{w\to 0} q(w) = q(0).$$

This means that for $|w|$ small enough [2], $|q(w) - q(0)| < t$ (we will choose t later).
c) Bound $|E(w)|$ in terms of r, k_0, t for $|w|$ small enough.

2. i.e. $\exists\, d > 0$ s.t. $\forall w \in \mathbb{C}$ with $|w| < d$, we have the following...

2pts

Let $w = re^{i\theta}$ (so $r = |w|$). Then :

$$|E(w)| = |w^{k_0}||q(w) - q(0)| = r^{k_0}|q(w) - q(0)| < r^{k_0}t \quad \text{for } |w| \text{ small enough.}$$

d) Show that $|p(z_0 + w)| \leq |p(z_0) + w^{k_0}q(0)| + |E(w)|$

2pts

We have $p(z_0 + w) = P(w) = p(z_0) + w^{k_0}q(0) + E(w)$, so by triangle inequality :

$$|p(z_0 + w)| = |p(z_0) + w^{k_0}q(0) + E(w)| \leq |p(z_0) + w^{k_0}q(0)| + |E(w)|.$$

e) Combining various previous results, show that $|p(z_0 + w)| < R - r^{k_0}(S - t)$ for $|w|$ small enough.

3pts

From the previous steps, we let :

- $p(z_0) = Re^{i\alpha}$
- $q(0) = Se^{i\beta}$
- $w = re^{i\theta}$

Choosing θ carefully, this gave :

- $p(z_0 + w) = P(w) = p(z_0) + w^{k_0}q(0) + E(w)$.
- $|E(w)| < r^{k_0}t$ for $|w|$ small enough.
- $|p(z_0) + w^{k_0}q(0)| = R - r^{k_0}S$

Combining everything :

$$|p(z_0 + w)| \leq |p(z_0) + w^{k_0}q(0)| + |E(w)| < (R - r^{k_0}S) + r^{k_0}t = R - r^{k_0}(S - t).$$

f) Choosing t carefully, show two contradicting statements, and conclude that every non-constant polynomial $p(z)$ has at least one root.

3pts

Choose $t = S/2 > 0$. Then for $r > 0$ small enough, we have :

$$|p(z)| = |p(z_0 + w)| \leq R - r^{k_0}(S - t) = R - r^{k_0}\frac{S}{2} < R = |p(z_0)|.$$

But this contradicts the definition of z_0 as a global minimum of $|p(z)|$. Hence, our assumption that $|p(z_0)| > 0$ is false. Therefore, every non-constant polynomial $p(z)$ has at least one root in $\mathbb{C}$.

5. By recurrent factorization, show that polynomial of degree n have exactly n roots.

3pts

Let $p(z)$ be a polynomial of degree $n \geq 1$. By the previous result, $p(z)$ has at least one root $z_1 \in \mathbb{C}$. Factor out $(z - z_1)$:

$$p(z) = (z - z_1)p_1(z), \quad \deg(p_1) = n - 1.$$

By induction on the degree, $p_1(z)$ has exactly $n - 1$ roots in $\mathbb{C}$. Hence, $p(z)$ has exactly n roots in $\mathbb{C}$.

6. From now on, it can be assumed that

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

can be rewritten as

$$p(z) = a_n \prod_{k=1}^{n} (z - z_k) \quad \text{with } a_n \in \mathbb{C}, z_k \in \mathbb{C}.$$

Moreover, if $a_n = 1$, p is called "monic" (the leading coefficient is 1).

a) Show by induction that if p is monic, then

$$a_0 = (-1)^n \prod_{k=1}^{n} z_k.$$

4pts

Let p be monic, write it as

$$p(z) = \prod_{k=1}^{n} (z - z_k).$$

Base case : $n = 1$, $p(z) = z - z_1$, so $a_0 = -z_1 = (-1)^1 z_1$. True.
Inductive step : Assume the result holds for degree $n - 1$. For n,

$$p(z) = (z - z_n) \prod_{k=1}^{n-1} (z - z_k).$$

The constant term of p is

$$a_0 = (-z_n) \prod_{k=1}^{n-1} (-z_k) = (-1)^n \prod_{k=1}^{n} z_k.$$

Hence, by induction,

$$\boxed{a_0 = (-1)^n \prod_{k=1}^{n} z_k}.$$

b) Show by induction that if p is monic, then

$$a_{n-1} = -\sum_{k=1}^{n} z_k.$$

6pts

Let p be monic, write it as

$$p(z) = \prod_{k=1}^{n} (z - z_k).$$

We want to prove by induction that

$$a_{n-1} = -\sum_{k=1}^{n} z_k.$$

Base case : $n = 1$, $p(z) = z - z_1$, so $a_0 = -z_1$. True.
Inductive step : Assume the result holds for degree $n - 1$. Write

$$p(z) = (z - z_n) \prod_{k=1}^{n-1} (z - z_k) \quad \text{where } q(z) = \prod_{k=1}^{n-1} (z - z_k)$$

is monic of degree $n - 1$.
Denote the coefficient of z^{n-1} in $p(z)$ be a_{n-1}, and the coefficient of z^{n-2} in $q(z)$ be b_{n-2}.
Expanding, we have

$$p(z) = (z - z_n)q(z) = z\,q(z) - z_n q(z)$$

.

- The coefficient of z^{n-1} in $z\,q(z)$ is b_{n-2}.
- The coefficient of z^{n-1} in $-z_n q(z)$ is $-z_n \cdot 1 = -z_n$, because $q(z)$ is monic of degree $n - 1$.
- The remaining terms of lower degree do not contribute to z^{n-1}.

Thus, the coefficient of z^{n-1} in $p(z)$ is :

$$a_{n-1} = \underbrace{-z_n}_{\text{from } z_n q(z)} + \underbrace{b_{n-2}}_{\text{from } zq(z)} .$$

Now, applying the induction hypothesis on q, we get

$$b_{n-2} = -\sum_{k=1}^{n-1} z_k \quad \text{so, finally,} \quad a_{n-1} = -\sum_{k=1}^{n} z_k.$$

This completes the proof by induction.

In part I, we found that there is an analytic solution to find the root for polynomials of degree 1, 2, 3, *and* 4.
In part II, we found that polynomials of degree n *must have exactly* n *roots.*
Hence, it would be reasonable to conjecture that there exists a general formula to find the root of a polynomial of any degree, right ?

III - Link with Group Theory

1. Consider two objects labeled 1 and 2. We call (1 2) the transformation (or permutation) that swaps the two objects, and (1) the identity (no swapping). Performing two transformations (two permutations) in turns will be denoted $\star$.
Informally, suppose we have two balls : one white (denote it "W"), and one black (denoted "B"). The initial state is (W, B). Then, (1) is the operation that does not change the state : $(1) \cdot (W, B) = (W, B)$. While (1 2) is the operation that swaps the two objects : $(1\ 2) \cdot (W, B) = (B, W)$.
a) Compute the following compositions :

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

2pts

i) $(1\ 2) \star (1\ 2) = (1)$; Indeed, swapping twice returns each object to its original position.
ii) $(1) \star (1\ 2) = (1\ 2)$; The identity permutation leaves the permutation unchanged.
iii) $(1\ 2) \star (1) = (1\ 2)$; Composing with the identity again leaves the permutation unchanged.
iv) $(1) \star (1) = (1)$; The composition of the identity with itself is the identity.

b) A set S equipped with an operation $\cdot$ is called a *group* if the following properties are satisfied :

— **Closure :** $\forall a, b \in S \quad a \cdot b \in S$
— **Associativity :** $\forall a, b, c \in S \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
— **Identity :** $\exists\ e \in S$ s.t. $\forall a \in S, a \cdot e = e = e \cdot a$
— **Inverse :** $\forall a \in S, \exists\ a^{-1} \in S$ s.t. $a \cdot a^{-1} = e = a^{-1} \cdot a$

Show that the set $\{(1), (1\ 2)\}$ together with the operation $\star$ forms a group (called S_2).
Take note that in here, (1) *and* (1 2) *are transformations or functions (formally called permutations), but are seen as elements of the group, i.e.* $(1), (1\ 2) \in S_2$.

4pts

- Closure. From part (a) we computed :

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

In each case the result lies in S, so S is closed under $\star$.
- Associativity. Composition of functions (and hence of permutations) is associative, so $\star$ is associative on S.
- Identity element. The permutation (1) acts as the identity for composition ($e=(1)$) :

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

- Inverses. We check that every element of S has an inverse in S :

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

and

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

Thus each element has an inverse in S.

c) A group is called *abelian* if the operation commutes, that is, $\forall a,b\in S,\quad a\cdot b=b\cdot a$.
Is S_2 commutative ? Justify your answer.

4pts

For the group $S_2=\{(1),(1\ 2)\}$, we check all possible products :

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

In each case, the order of composition does not affect the result, so the group S_2 is commutative (abelian).

d). Let $x^2+px+q=0$ be a quadratic equation with roots r_1 and r_2.

i) Write the roots r_1 and r_2 using the quadratic formula.

2pts

By the quadratic formula :

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

ii) The two roots can be seen as the objects moved around by the permutations (1) and (1 2) (i.e. S_2). Find one quantity involving r_1 and r_2 that is unchanged under this permutation.

2pts

The action of $S_2=\{(1),(1\ 2)\}$ either leaves the pair (r_1,r_2) unchanged or swaps the two roots ; i.e. :

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

A quantity is unchanged under this swap if it is *symmetric* in r_1 and r_2. For example, the sum r_1+r_2 is invariant, because

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

(Equivalently, by Vieta's formulas, $r_1+r_2=-p$, which does not depend on the ordering of the roots.)

2. Consider now three objects labeled 1, 2, and 3. The set of all permutations of $\{1,2,3\}$ equipped with the operation $\star$ (composition) is called S_3. We define the following permutations :

— We call (1) the permutation that does nothing.
— We call (1 2) the permutation that swaps objects 1 and 2.

— We call (1 3) the permutation that swaps objects 1 and 3.
— We call (2 3) the permutation that swaps objects 2 and 3.
— We call (1 2 3) the permutation that rotates objects $1 \to 2$, $2 \to 3$, and $3 \to 1$.
— We call (1 3 2) the permutation that rotates objects 1, 2, and 3 in the other direction ($1 \to 3$, $3 \to 2$, and $2 \to 1$).

a) Copy and complete the following table (called a *Cayley table*) describing the operation $\star$ on 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) Is the group S_3 abelian ? Justify your answer.

2pts

No, S_3 is *not* abelian. It suffices to find two elements that do not commute.

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

Now,

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

so, the operation is not commutative. Hence S_3 is not abelian.

The *order* of a, denoted $\text{ord}(a)$, is the smallest positive integer n such that $a^n = e$, where e is the identity element. *(If no such positive integer exists, then g is said to have infinite order.)*
c) What is the order of (1 2 3) ? What is the order of (2 3) ?

3pts

Order of (1 2 3)**.**

2pts

The permutation (1 2 3) cycles the elements as $1 \to 2$, $2 \to 3$, $3 \to 1$. Computing its powers,

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

Since the identity appears for the first time at the third power, we have $\text{ord}(1\ 2\ 3) = 3$.
Order of (2 3)**.**

1pt

The permutation (2 3) is a transposition. Computing its square, $(2\ 3)^2 = (1)$. Thus the smallest positive integer n such that $(2\ 3)^n = (1)$ is $n = 2$, and therefore $\text{ord}(2\ 3) = 2$.

d) A non-empty subset H of a group G is called a *subgroup* if it satisfies the following properties :
— it contains the identity element (i.e. $e \in H$) ;
— it is closed under the group operation (i.e. $\forall a, b \in H, a \cdot b \in H$) ;

— it is closed under taking inverses (i.e. $\forall a \in H, a^{-1} \in H$).

Let $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\} \subset S_3$.
Show that H is a subgroup of S_3.

3pts

- Identity.
The identity element of S_3 is (1), and clearly $(1) \in H$.
- Closure under $\star$.
Let $a, b \in H$. We check that $a \star b \in H$ by computing the products among the three elements. Using that (1) is the identity and that

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

similarly

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

we see that every product of two elements of H is again one of

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

hence lies in H. Therefore H is closed under $\star$.
- Closure under inverses.
We have

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

Also, since $(1\ 2\ 3)^3 = (1)$, we get

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

and similarly

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

Thus H is closed under inverses.

Since H contains the identity, is closed under the group operation $\star$, and is closed under taking inverses, H is a subgroup of S_3.

3. Consider now five objects labeled $1, 2, 3, 4, 5$. The set of all permutations of these five objects equipped with the composition operation $\star$ is called S_5. A cycle $(a_1\ a_2\ \dots\ a_k)$ sends a_i to a_{i+1} for $i = 1, \dots, k-1$, sends a_k to a_1, and fixes all other elements.
a) How many different permutations are there in S_5 ? This is called the size of S_5, and is denoted $|S_5|$.

2pts

A permutation of the set $\{1, 2, 3, 4, 5\}$ is a bijection from the set to itself. To construct a permutation, we may choose the image of each element :

— there are 5 choices for where 1 is sent,
— once this is chosen, there are 4 remaining choices for where 2 is sent,
— then 3 choices for where 3 is sent,
— then 2 choices for where 4 is sent,
— and finally 1 choice for where 5 is sent.

Multiplying all, the total number of permutations is $5 \times 4 \times 3 \times 2 \times 1 = 5!$. Thus $|S_5| = 5! = 120$.

b) Simple permutations.
i) Give an example of a permutation in S_5 with order 2.
ii) Give an example of a permutation in S_5 with order 3.
iii) Give an example of a permutation in S_5 with order 5.
iv) Give an example of a permutation in S_5 with order 6.

4pts

i) **Order 2.**
Any transposition has order 2. For example, $(1\ 2)$ satisfies $(1\ 2)^2 = (1)$, so $\mathrm{ord}(1\ 2) = 2$.

ii) **Order 3.**
Any 3-cycle has order 3. For example, $(1\ 2\ 3)$ satisfies $(1\ 2\ 3)^3 = (1)$, so $\mathrm{ord}(1\ 2\ 3) = 3$.

iii) **Order 5.**
A 5-cycle has order 5. For example, $(1\ 2\ 3\ 4\ 5)$ satisfies $(1\ 2\ 3\ 4\ 5)^5 = (1)$, so $\mathrm{ord}(1\ 2\ 3\ 4\ 5) = 5$.

iv) **Order 6.** ***Remark :*** *For a permutation written as a product of* disjoint cycles*, its order is the least common multiple of the lengths of those cycles.*
Consider a product of disjoint cycles of lengths 3 and 2, for example $(1\ 2\ 3)(4\ 5)$. The order is $\mathrm{lcm}(3, 2) = 6$, so this permutation has order 6.

c) Is the group S_5 abelian ? Justify your answer.

2pts

No, S_5 is *not* abelian.
To justify this, it suffices to find two permutations in S_5 that do not commute :
Let $\sigma = (1\ 2)$, and $\tau = (2\ 3)$. Compute the compositions :

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

Since $(1\ 2\ 3) \neq (1\ 3\ 2)$, we have $\sigma \star \tau \neq \tau \star \sigma$. Therefore the operation is not commutative, and hence S_5 is not abelian.

d) A *transposition* is a permutation that swaps exactly two objects and leaves all others unchanged.

i) Write the cycle $(1\ 2\ 3)$ as the product of two transpositions.

1pt

We claim $(1\ 2\ 3) = (1\ 3)(1\ 2)$. Indeed, applying the right-hand side first :

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

so overall $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, which is exactly $(1\ 2\ 3)$.

ii) Write the cycle $(1\ 2\ 3\ 4)$ as a product of transpositions (this cycle send $1 \to 2$, $2 \to 3$, $3 \to 4$, and $4 \to 1$).

2pts

We claim $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$.. Indeed, applying the right-hand side first :

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

so overall $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, and $4 \mapsto 1$, which is exactly $(1\ 2\ 3\ 4)$.

iii) Show that a general cycle $(1\ 2\ \ldots\ k)$ can be written as a product of transpositions of the form $(a_1\ a_i)$ (this cycle send $1 \to 2$, $2 \to 3$, ..., $(k-1) \to k$, $k \to 1$,).

3pts

We will show that for $k \geq 2$, $(1\ 2\ \ldots\ k) = (1\ k)(1\ k-1)\cdots(1\ 3)(1\ 2)$.
Let $\sigma = (1\ k)(1\ k-1)\cdots(1\ 2)$. We compute $\sigma(i)$:

- For $i = 1$: under the rightmost transposition $(1\ 2)$ we get $1 \mapsto 2$, and none of the remaining transpositions moves 2, so $\sigma(1) = 2$.
- In fact, for $1 \leq i \leq k-1$: the transposition $(1\ i)$ sends $i \mapsto 1$, and then the next transposition to the left, namely $(1\ i+1)$, sends $1 \mapsto i+1$. No other transposition affects $i+1$, hence $\sigma(i) = i+1$.
- For $i = k$: the transposition $(1\ k)$ sends $k \mapsto 1$, and no later transposition (to the left) changes 1 into something else, so $\sigma(k) = 1$.
- Any element not in $\{1, 2, \ldots, k\}$ is fixed by every transposition, hence is fixed by σ.

Therefore σ acts as $1 \mapsto 2 \mapsto \cdots \mapsto k \mapsto 1$, so $\sigma = (1\ 2\ \ldots\ k)$.

iv) Show that a general permutation can be written as a product of transpositions.

4pts

By relabeling the argument in (iii), we obtain the standard decomposition

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

which is a product of transpositions.
Let $\sigma \in S_n$ be any permutation. We will partition $\{1, 2, \dots, n\}$ into cycles determined by the action of σ. Pick an element a_1. Consider its orbit under σ :

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

Since the set is finite, there exist integers $i < j$ with $\sigma^i(a_1) = \sigma^j(a_1)$. Applying σ^{-i} gives $a_1 = \sigma^{j-i}(a_1)$. Let k be the smallest positive integer such that $\sigma^k(a_1) = a_1$. Then the elements $a_1,\ a_2 = \sigma(a_1),\ a_3 = \sigma^2(a_1),\ \dots,\ a_k = \sigma^{k-1}(a_1)$ are all distinct, and on this set σ acts by $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$, so σ restricts to the cycle $(a_1\ a_2\ \cdots\ a_k)$.
If this cycle does not include all elements of $\{1, \dots, n\}$, choose b_1 not in $\{a_1, \dots, a_k\}$ and repeat the same construction to obtain another cycle. Continuing, we eventually exhaust all elements. The cycles obtained are disjoint because they come from disjoint orbits, and on each orbit σ agrees with the corresponding cycle, while fixing all elements outside that orbit. Therefore σ equals the product of these disjoint cycles.
Since each cycle is a product of transpositions by the formula above, it follows that any permutation is a product of transpositions.

4. Recall that S_5 is the group of all permutations of five objects. A permutation is called *even* if it can be written as a product of an even number of transpositions. The set of all even permutations of S_5 is called the *alternating group* A_5.
a) Show that A_5 is a subgroup of S_5.

4pts

- Identity.
The identity permutation (1) can be written as a product of 0 transpositions, and 0 is even. Hence $(1) \in A_5$.
- Closure under composition.
Let $\sigma, \tau \in A_5$. Then there exist transpositions $t_1, \dots, t_{2m}$ and $s_1, \dots, s_{2n}$ such that

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

Then

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

which is a product of $2m + 2n$ transpositions. Since $2m + 2n$ is even, we have $\sigma \star \tau \in A_5$.
- Closure under inverses.
Let $\sigma \in A_5$ with $\sigma = t_1 t_2 \cdots t_{2m}$ a product of $2m$ transpositions. Taking inverses and using $(ab)^{-1} = b^{-1}a^{-1}$ gives $\sigma^{-1} = (t_1 t_2 \cdots t_{2m})^{-1} = t_{2m}^{-1} \cdots t_2^{-1} t_1^{-1}$.
But each transposition is its own inverse, $t_i^{-1} = t_i$, so $\sigma^{-1} = t_{2m} \cdots t_2 t_1$, which is again a product of $2m$ transpositions, hence an even number. Therefore $\sigma^{-1} \in A_5$.

Since A_5 contains the identity, is closed under the group operation, and is closed under inverses, it is a subgroup of S_5.

b) Show that exactly half of the permutations in S_5 are even. Deduce the size of $|A_5|$.

4pts

Let $\tau = (1\ 2)$, a transposition ; define a map $f : S_5 \to S_5, \qquad f(\sigma) = \tau \star \sigma = \tau\sigma$.
Claim 1 : f is a bijection.
Indeed, f is its own inverse, since $\tau^{-1} = \tau$:

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

Hence f is a bijection.
Claim 2 : f swaps parity (even $\leftrightarrow$ odd).
If σ is even, write σ as a product of $2m$ transpositions. Then $f(\sigma) = \tau\sigma$ is a product of $2m + 1$ transpositions, hence is odd. Conversely, if σ is odd (a product of $2m + 1$ transpositions), then $\tau\sigma$ is a product of $2m + 2$ transpositions, hence even.

Thus f gives a bijection from the set of even permutations to the set of odd permutations. Therefore the number of even permutations equals the number of odd permutations, so *exactly half* of the elements of S_5 are even.

Since $|S_5| = 5! = 120$, we conclude $|A_5| = \frac{|S_5|}{2} = 60$.

5. Let G be a group. Two elements $g, h \in G$ are said to be in the same class if there exists an element $x \in G$ such that $h = xgx^{-1}$.. The set of all elements related to g in this way is called the *class* of g.
a) Show that the identity element forms a class by itself.

1pts

For any $x \in G$, $xex^{-1} = e$, so the conjugate of e is always e. Hence the class of e is $\{xex^{-1} : x \in G\} = \{e\}$ (i.e. it contains only the identity).

b) Explain why an element cannot belong to two different classes at the same time.

4pts

Define a relation $\sim$

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

This is the usual *conjugacy* relation, and is an equivalence relation :

- Reflexive : $g = ege^{-1}$, so $g \sim g$.
- Symmetric : if $h = xgx^{-1}$ then $g = x^{-1}hx$, so $h \sim g$.
- Transitive : if $h = xgx^{-1}$ and $k = yhy^{-1}$ then $k = y(xgx^{-1})y^{-1} = (yx)g(yx)^{-1}$, so $g \sim k$.

Therefore the classes are exactly the equivalence classes of $\sim$, and equivalence classes are either identical or disjoint. Hence an element cannot lie in two different classes at once.

c) Compare $|G|$ with the sum of the sizes of all the classes.

2pts

Since conjugacy classes are disjoint and their union is all of G, they form a partition of G.
Thus,

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

where the sum runs over all conjugacy classes $\mathcal{C}$ of G.

6. A subgroup H of a group G is called *invariant* (or *normal*) if for every $g \in G$ and every $h \in H$, the element ghg^{-1} also belongs to H. In this case, we write $H \triangleleft G$.

a) Let H be an invariant subgroup of G, and let $h \in H$. Explain why the entire class of h must be contained in H.

4pts

Suppose $H \triangleleft G$. Let $h \in H$ and let $x \in G$ be arbitrary. Then, by the defining property of an invariant subgroup, $xhx^{-1} \in H$. Thus every conjugate of h by an element of G belongs to H. Equivalently, the entire conjugacy class of h in G is contained in H.

b) Conclude that any invariant subgroup must be a union of entire classes together with the identity.

2pt

Follows directly from i) and the fact that the identity element must belong to H (by definition of H being a subgroup).

7. We will prove the **Lagrange's Theorem** : the order of any subgroup must divide the order of the group.
Supose G is a finite group and H is a subgroup of G.

a) Let $g \in G$, define the set $gH = \{gh \mid h \in H\}$. Explain why $gH \subseteq G$.

1pt

Since $g \in G$ and $H \subseteq G$, for every $h \in H$ we have $h \in G$. Because G is a group, it is closed under the group operation, so the product gh belongs to G. Therefore every element of the form gh lies in G, which shows that $gH \subseteq G$.

b) Show that if $g_1H = g_2H$, then $g_2^{-1}g_1 \in H$. Conversely, show that if $g_2^{-1}g_1 \in H$, then $g_1H = g_2H$.

2pts

First assume that $g_1H = g_2H$. Since $g_1 \in g_1H$, we have $g_1 \in g_2H$, so there exists $h \in H$ such that $g_1 = g_2h$. Multiplying on the left by g_2^{-1} gives $g_2^{-1}g_1 = h \in H$.
Conversely, assume that $g_2^{-1}g_1 \in H$. Then there exists $h \in H$ such that $g_2^{-1}g_1 = h$, so $g_1 = g_2h$. For any $h' \in H$ we have $g_1h' = g_2(hh') \in g_2H$, since H is a subgroup and hence closed under multiplication. Thus $g_1H \subseteq g_2H$. By symmetry, the reverse inclusion also holds, and therefore $g_1H = g_2H$.

c) Deduce that for any $g_1, g_2 \in G$, the sets g_1H and g_2H are either equal or disjoint.

2pts

If $g_1H = g_2H$, we are done. Otherwise, suppose that $g_1H \cap g_2H \neq \varnothing$. Then there exists an element $x \in G$ such that $x = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$. Rewriting gives $g_2^{-1}g_1 = h_2h_1^{-1} \in H$, since H is a subgroup. By the previous result, this implies that $g_1H = g_2H$. Therefore, if $g_1H \neq g_2H$, the intersection must be empty, and the two sets are disjoint.

d) Define the function $f : H \to gH \quad$ by $\quad f(h) = gh$. Show that f is a bijection.

2pts

We first show that f is injective. Suppose that $f(h_1) = f(h_2)$ for some $h_1, h_2 \in H$. Then $gh_1 = gh_2$, and multiplying on the left by g^{-1} gives $h_1 = h_2$. Thus f is injective.
Next, we show that f is surjective. By definition of gH, every element $x \in gH$ can be written as $x = gh$ for some $h \in H$. Then $x = f(h)$, so every element of gH is in the image of f. Thus f is surjective.
Since f is both injective and surjective, it is a bijection.

e) Deduce that every set of the form gH has exactly $|H|$ elements.

2pts

From the previous question, the map $f : H \to gH$ defined by $f(h) = gh$ is a bijection. A bijection pairs each element of H with exactly one element of gH, and vice versa. Therefore H and gH have the same number of elements, so $|gH| = |H|$.

f) Explain why G can be written as a disjoint union of k distinct sets of the form gH, each containing exactly $|H|$ elements, for some integer k.

2pts

Every element $g \in G$ belongs to the left coset gH (since $g = g \cdot e$ and $e \in H$), so the union of all sets of the form gH is equal to G. From the previous result, any two cosets g_1H and g_2H are either equal or disjoint, so the distinct cosets form a partition of G. Since G is finite, there are only finitely many distinct cosets; call their number k. Each coset has $|H|$ elements, so G is a disjoint union of k distinct sets of the form gH, each of size $|H|$.

g) Conclude that $|H|$ divides $|G|$.

1pt

Since G is a disjoint union of k distinct left cosets of H, and each coset has exactly $|H|$ elements, we have $|G| = k\,|H|$ for some integer k. Therefore $|H|$ divides $|G|$.

A group with no proper invariant subgroup (no other invariant subgroup than itself and $\{e\}$) is called *simple*.
f) The class sizes of A_5 are $1, 12, 12, 20, 15$. Conclude that A_5 is simple.

4pts

Let $H \trianglelefteq A_5$ with $e \in H$. Since H is invariant, it must be a union of conjugacy classes, hence its size is

$$|H| = 1 + (\text{a sum of } 12, 12, 20, 15).$$

Thus the possible values are :

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

Since H is a subgroup, its size $|H|$ must divide $|A_5| = 60$. Therefore, the possible sizes are $|H| = 1$ and $|H| = 60$.

8. A group G is called *solvable* if its *derived series* eventually reaches the trivial subgroup :

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

where $[G, G]$ is the subgroup generated by all *commutators* $[g, h] = ghg^{-1}h^{-1} \quad (g, h \in G)$, that is :

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

G is solvable if there exists n such that $G^{(n)} = \{e\}$.
The goal of this question is to show that S_5 is not solvable.

a) Show that for any group G, the commutator subgroup $[G, G]$ is a *normal* subgroup of G.

3pts

Recall that $[G, G]$ is generated by all commutators $[a, b] = aba^{-1}b^{-1}$ with $a, b \in G$. Let $g \in G$ and let $[a, b]$ be a commutator. Then

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

which is again a commutator of elements of G. Thus $g[a, b]g^{-1} \in [G, G]$. Since conjugation preserves products, the conjugate of any product of commutators is again in $[G, G]$. Therefore $[G, G]$ is normal in G.

The quotient group $G/[G, G]$ is the set of all left cosets of the commutator subgroup $[G, G]$ in G :

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

The group operation is defined by

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

for all $g, h \in G$. This operation is well defined because $[G, G]$ is a normal subgroup of G.
b) Show that the quotient group $G/[G, G]$ is abelian.

4pts

Let $g, h \in G$ and consider their cosets in $G/[G, G]$. We have

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

Now note that

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

With $[g, h] \in [G, G]$, we see that gh and hg differ by multiplication by an element of $[G, G]$. By definition of cosets, two elements of G belong to the same coset of $[G, G]$ if and only if their product differs by an element of $[G, G]$. Thus

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

since multiplying by an element of $[G, G]$ does not change the coset.
Therefore

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

for all cosets, so $G/[G, G]$ is abelian.

c) Deduce that if G is *not* abelian, then $[G, G] \neq \{e\}$.

2pts

Assume for contradiction that $[G,G]=\{e\}$. Then the quotient group $G/[G,G]$ is just $G/\{e\}\cong G$. But we proved that $G/[G,G]$ is abelian, so G would be abelian as well, contradicting the assumption. Therefore, if G is not abelian, then $[G,G]\neq\{e\}$.

d) Using previous parts, deduce that $A_5^{(1)}=[A_5,A_5]$ is a *nontrivial normal* subgroup of A_5.

1pt

Since A_5 is not abelian (previous part), we have $[A_5,A_5]\neq\{e\}$. Also, for any group G, the commutator subgroup $[G,G]$ is normal in G (previous part), so $[A_5,A_5]\trianglelefteq A_5$. Therefore $A_5^{(1)}=[A_5,A_5]$ is a nontrivial normal subgroup of A_5.

e) Conclude that $[A_5,A_5]=A_5$.

1pt

From the previous result, $[A_5,A_5]$ is a nontrivial normal subgroup of A_5. But A_5 has no proper nontrivial normal subgroups, so the only possibility is $[A_5,A_5]=A_5$.

f) Conclude that A_5 is not solvable.

1pt

We have shown that $A_5^{(1)}=[A_5,A_5]=A_5$. Hence $A_5^{(2)}=[A_5^{(1)},A_5^{(1)}]=[A_5,A_5]=A_5$, and by induction $A_5^{(n)}=A_5$ for all $n\geq 1$. Therefore the derived series never reaches $\{e\}$, so there is no n with $A_5^{(n)}=\{e\}$. Thus A_5 is not solvable.

g) Show by induction on n that if G is solvable and $H\leq G$, then the derived series satisfies $H^{(n)}\leq G^{(n)}$ for all n.

3pts

For $n=0$, we have $H^{(0)}=H\leq G=G^{(0)}$.

Assume $H^{(n)}\leq G^{(n)}$ for some $n\geq 0$.
Then every commutator of elements of $H^{(n)}$ is also a commutator of elements of $G^{(n)}$. Hence the subgroup generated by these commutators satisfies

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

Thus the statement holds for $n+1$.
By induction, $H^{(n)}\leq G^{(n)}$ for all $n\geq 0$.

h) Conclude that S_5 is not solvable.

2pts

Assume for contradiction that S_5 is solvable. Since $A_5\leq S_5$, the previous result implies $A_5^{(n)}\leq S_5^{(n)}$ for all n. Because S_5 is solvable, there exists n such that $S_5^{(n)}=\{e\}$, hence $A_5^{(n)}=\{e\}$ as well. This would mean that A_5 is solvable, contradicting the fact that A_5 is not solvable. Therefore S_5 is not solvable.

*It can be shown that a polynomial $f(x)$ is **solvable by radicals** (that is, its roots can be expressed using a finite combination of arithmetic operations and radicals) if and only if the symmetry group of its roots—called its **Galois group** $G=\mathrm{Gal}(f/K)$—is a **solvable group**.*
In this exam, you proved that the symmetric group S_5 is not solvable. For a general polynomial of degree 5, the symmetry group of its roots is S_5. Therefore, there cannot exist a general formula (in radicals) for the roots of a polynomial of degree 5.
More generally, it can be shown that the symmetric groups S_n are not solvable for all $n\geq 5$. This implies that there is no general formula by radicals for the roots of a polynomial of degree greater than four.
This explains why explicit formulas exist for quadratic, cubic, and quartic equations, but not for equations of degree five or higher.

IV - To the Glory of Galois

1. Derive a general formula for solving quintic equations by radicals. Good luck.

1000pts