L'EVARISTE

Morning Exam

Duration: 2 hours

Mobile phones, tablets, computers, smart watches, and all electronic devices for communication or storage, as well as any documents, are prohibited.

Non-programmable calculators (middle-school type) or calculators in exam mode are allowed.

*The quality of the writing is an **important** factor in the evaluation of the papers. Humility is welcome in the reasoning. You may answer the questions in any order.*

ALBERTSCHOOL MINES PARIS | PSL

D E Shaw & Co

Reminders and notation:

We use the following logical quantifiers and connectives:

$\neg$	negation
$\forall$	for all
$\exists$	there exists
$\wedge$	conjunction (and)
$\vee$	disjunction (or)
$\Longrightarrow$	implication (if ... then ...)
$\Longleftrightarrow$	equivalence (if and only if)

We denote by $\mathbb{C}$ the set of *complex numbers*. We say that $z \in \mathbb{C}$ if there exist $x, y \in \mathbb{R}$ such that

$$z = x + iy,$$

where the *imaginary unit* i satisfies $i^2 = -1$. We call x the *real part* of z, denoted $\Re(z)$, and y its *imaginary part*, denoted $\Im(z)$. We also call the *conjugate* of z the complex number defined by

$$\overline{z} = x - iy,$$

and we call the *modulus* of z the nonnegative real number defined by

$$\sqrt{x^2 + y^2}.$$

I – Warm-up

In this section, let $a, b, c, d \in \mathbb{R}$. Assume $a \neq 0$.

1. a) [·/**1**] Solve the equation $ax + b = 0$.
   b) [·/**1**] Use your formula to solve $5x + 7 = 0$.
2. a) [·/**8**] By writing the quadratic expression in canonical form, solve
   $$ax^2 + bx + c = 0.$$
   b) Solve the following equations:
   i) [·/**2**] $x^2 + x - 6 = 0$
   ii) [·/**2**] $x^2 - 24x + 143 = 0$
   iii) [·/**2**] $x^4 - 5x^2 + 6 = 0$
   iv) [·/**2**] $(e^x)^2 - 5e^x + 6 = 0$
3. [·/**3**] Consider the equation
   $$ax^3 + bx^2 + cx + d = 0.$$
   Justify that there exist $a', b', c' \in \mathbb{R}$ such that this equation is equivalent to
   $$x^3 + a'x^2 + b'x + c' = 0.$$
4. [·/**3**] By making the change of variable
   $$x = y - \frac{a'}{3},$$
   show that there exist $p, q \in \mathbb{R}$ such that the previous equation is equivalent to
   $$y^3 + py + q = 0.$$
5. a) [·/**3**] Setting $y = u + v$, rewrite the equation $y^3 + py + q = 0$ in terms of u and v.
   b) [·/**3**] By imposing the condition
   $$uv = -\frac{p}{3},$$
   make explicit an equation relating u^3, v^3 and q.
6. Consider the following equation in the variable z:
   $$(z - u^3)(z - v^3) = 0.$$
   a) [·/**4**] Rewrite this equation with coefficients expressed in terms of p and q.
   b) [·/**4**] Express z in terms of p and q.
   Hint: you may use the formula obtained in Question 2.
   c) [·/**2**] Assuming that the two solutions of the equation in z are u^3 and v^3, make u and v explicit.
7. [·/**2**] Deduce an expression for y in terms of p and q.
8. [·/**6**] We admit that one of the solutions of
   $$y^3 + py + q = 0$$
   is given by
   $$y = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$
   Solve the equation
   $$x^3 + 9x^2 + 33x + 25 = 0.$$
   Hint: after finding one root, factor, then use the quadratic formula.

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

II – Fundamental Theorem of Algebra

1. a) [·/**1**] Show that
$$\forall z \in \mathbb{C}, \quad \Re(z) \leqslant |z| = |\overline{z}|.$$
b) [·/**1**] Show that
$$\forall z \in \mathbb{C}, \quad |z|^2 = z\overline{z}.$$
c) [·/**1**] By computing $|zw|^2$, show that
$$\forall z, w \in \mathbb{C}, \quad |zw| = |z|\,|w|.$$
d) [·/**4**] By computing $|z+w|^2$, show that
$$\forall z, w \in \mathbb{C}, \quad |z+w| \leqslant |z| + |w| \qquad \text{(Triangle inequality)}.$$
e) [·/**2**] Using the triangle inequality, justify that
$$\forall z, w \in \mathbb{C}, \quad |z| - |w| \leqslant |z+w|.$$

The goal of this section is to show that every polynomial
$$P(z) = \sum_{k=0}^{n} a_k z^k \qquad \text{where } a_k \in \mathbb{C},$$
has exactly n complex roots (counted with multiplicity).

2. a) [·/**4**] Show that
$$\lim_{|z|\to+\infty} |p(z)| = +\infty.$$
b) [·/**1**] Deduce that there exists $R > 0$ such that
$$\forall z \in \mathbb{C},\ |z| > R \ \Rightarrow\ |p(z)| > |p(0)| + 1.$$
c) [·/**2**] Considering
$$D = \{\, z \in \mathbb{C} \mid |z| \leqslant R \,\},$$
show that $|p(z)|$ attains a global minimum on D.

3. Let z_0 be a point where this minimum is attained, i.e.
$$\forall z \in \mathbb{C}, \quad |p(z_0)| \leqslant |p(z)|.$$
Assume for contradiction that $|p(z_0)| > 0$.
Set $w = z - z_0$ and define $P(w) = p(z_0 + w)$. Write
$$P(w) = \sum_{k=0}^{n} b_k w^k.$$
a) [·/**1**] Express b_0 in terms of $p(z_0)$.
b) [·/**1**] Show that there exists an integer $k_0 \geqslant 1$ such that
$$P(w) = b_0 + w^{k_0} q(w),$$
where q is a polynomial satisfying $q(0) \neq 0$.

4. We use the approximation $w^{k_0} q(w) \approx w^{k_0} q(0)$ for small $|w|$. Write
$$p(z_0) = Re^{i\alpha}, \qquad q(0) = Se^{i\beta}, \qquad w = re^{i\theta}.$$
a) [·/**1**] Express w^{k_0} and $w^{k_0} q(0)$ in terms of r, S, β, θ.

b) [·/**3**] Find θ such that

$$\arg(w^{k_0}q(0)) \equiv \arg(p(z_0)) + \pi \pmod{2\pi}.$$

c) [·/**2**] Deduce the expression of $w^{k_0}q(0)$.

d) [·/**2**] Show that

$$|p(z_0) + w^{k_0}q(0)| < |p(z_0)|.$$

e) [·/**2**] Conclude a contradiction under the hypothesis $|p(z_0)| > 0$.

5. Define the error term

$$E(w) = w^{k_0}(q(w) - q(0)).$$

a) [·/**2**] Express $P(w)$ in terms of b_0, $w^{k_0}q(0)$, and $E(w)$.

b) [·/**2**] Justify that

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

c) [·/**2**] Bound $|E(w)|$ for $|w|$ small enough.

d) [·/**2**] Show that

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

e) [·/**3**] Conclude that p has at least one root.

6. [·/**3**] By iterative factorization, show that a polynomial of degree n has exactly n roots.

III - Discussion around group theory

1. Consider two objects labeled 1 and 2. We call (1) the identity permutation, and (1 2) the permutation that swaps the two objects. Composition of permutations is denoted by $\star$.

   We can represent the situation concretely: we have two balls, a white one (denoted W) and a black one (denoted B). The initial state is (W, B). The permutation (1) leaves the state unchanged, while (1 2) swaps the two balls.

   a) [·/**2**] Compute the following compositions:
   - $(1\ 2) \star (1\ 2)$
   - $(1) \star (1\ 2)$
   - $(1\ 2) \star (1)$
   - $(1) \star (1)$

   b) [·/**4**] Recall that a set S equipped with an operation $\cdot$ is called a group if it satisfies:
   - **Closure:** $\forall a, b \in S,\ a \cdot b \in S$;
   - **Associativity:** $\forall a, b, c \in S,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
   - **Identity element:** $\exists e \in S$ such that $\forall a \in S,\ a \cdot e = e \cdot a = a$;
   - **Inverse:** $\forall a \in S,\ \exists a^{-1} \in S$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

   Show that the set $\{(1), (1\ 2)\}$ equipped with $\star$ is a group, denoted S_2.

   c) [·/**4**] A group is called *abelian* if

   $$\forall a, b \in S, \quad a \cdot b = b \cdot a.$$

   Is the group S_2 abelian? Justify.

2. Now consider a quadratic equation

$$x^2 + px + q = 0$$

having two roots r_1 and r_2.

   a) [·/**2**] Write the roots r_1 and r_2 using the quadratic formula.

   b) [·/**2**] We can view r_1 and r_2 as two objects permuted by the group S_2. Find a quantity involving r_1 and r_2 that is invariant under permutation.

3. Now consider three objects labeled 1, 2, and 3. The set of all permutations of $\{1, 2, 3\}$ equipped with composition $\star$ is denoted S_3.

   Define the following permutations:

   - (1): identity;
   - (1 2), (1 3), (2 3): transpositions;
   - (1 2 3) and (1 3 2): 3-cycles.

   a) [·/**6**] Complete the Cayley table of 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)						

   b) [·/**2**] Is the group S_3 abelian? Justify.

   c) [·/**3**] The *order* of an element a, denoted $\mathrm{ord}(a)$, is the smallest integer $n \geqslant 1$ such that $a^n = e$. Determine the order of (2 3), then the order of (1 2 3).

4. Now consider five objects labeled $1, 2, 3, 4, 5$. The set of all permutations of these objects equipped with composition is denoted S_5.

   a) [·/**2**] How many permutations are there in S_5? Denote this number by $|S_5|$.

   b) [·/**4**] Give an example of a permutation in S_5:

      - of order 2;
      - of order 3;
      - of order 5;
      - of order 6.

   c) [·/**2**] Is the group S_5 abelian? Justify.

5. A *transposition* is any permutation that swaps exactly two elements and leaves the others fixed.

   a) [·/**1**] Write the cycle (1 2 3) as a product of transpositions.

   b) [·/**2**] Write the cycle (1 2 3 4) as a product of transpositions.

   c) [·/**3**] Show that a general cycle (1 2 ... k) can be written as a product of transpositions.

   d) [·/**4**] Show that any permutation can be written as a product of transpositions.

6. A permutation is called *even* if it can be written as a product of an even number of transpositions. The set of even permutations in S_5 is denoted A_5.

   a) [·/**4**] Show that A_5 is a subgroup of S_5.

   b) [·/**4**] Show that exactly half of the permutations in S_5 are even. Deduce $|A_5|$.

7. Two elements g, h of a group G are said to be *conjugate* if there exists $x \in G$ such that

$$h = xgx^{-1}.$$

   The set of elements conjugate to g is called the *conjugacy class* of g.

   a) [·/**1**] Show that the identity element forms a conjugacy class by itself.

   b) [·/**4**] Show that an element can belong to only one conjugacy class.

   c) [·/**2**] Compare $|G|$ with the sum of the sizes of all conjugacy classes.

8. A subgroup H of a group G is called *normal* if

$$\forall g \in G,\ \forall h \in H, \quad ghg^{-1} \in H.$$

We then write $H \triangleleft G$.

a) [·/**4**] Show that every conjugacy class of an element of H is contained in H.

b) [·/**2**] Deduce that a normal subgroup is a union of entire conjugacy classes.

9. Let G be a finite group and H a subgroup of G.

a) [·/**1**] Define $gH = \{gh \mid h \in H\}$ and show that $gH \subseteq G$.

b) [·/**2**] Show that $g_1H = g_2H$ if and only if $g_2^{-1}g_1 \in H$.

c) [·/**2**] Deduce that the two sets g_1H and g_2H are either equal or disjoint.

d) [·/**2**] Show that the map $h \longmapsto gh$ is a bijection from H to gH.

e) [·/**2**] Deduce that $|gH| = |H|$.

f) [·/**2**] Show that G is the disjoint union of k left cosets of H.

g) [·/**1**] Conclude that $|H|$ divides $|G|$ (Lagrange's Theorem).

10. We admit that the sizes of the conjugacy classes of A_5 are

$$1,\ 12,\ 12,\ 20,\ 15.$$

a) [·/**4**] Deduce that A_5 is a simple group.

11. The *derived series* of a group G is the sequence of subgroups defined by

$$G^{(0)} = G \quad \text{and} \quad G^{(n+1)} = [G^{(n)}, G^{(n)}] \qquad (n \in \mathbb{N}),$$

where, for any group H, we define

$$[H,H] = \left\{ \prod_{k=1}^{m} h_k h'_k h_k^{-1} h'^{-1}_k \;\middle|\; m \in \mathbb{N},\ h_k, h'_k \in H \right\}.$$

The group G is called *solvable* if there exists $n \in \mathbb{N}$ such that

$$G^{(n)} = \{e\}.$$

a) [·/**3**] Show that, for any group G, the subgroup $[G,G]$ is a normal subgroup of G.

b) [·/**4**] Define the quotient group

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

Show that the operation

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

is well-defined and that $G/[G,G]$ is a group.

c) [·/**4**] Show that the quotient group $G/[G,G]$ is abelian.

d) [·/**2**] Deduce that if G is not abelian, then $[G,G] \neq \{e\}$.

12. Now consider the alternating group A_5.

a) [·/**1**] Justify that A_5 is not abelian.

b) [·/**1**] Deduce that $A_5^{(1)} = [A_5, A_5]$ is a nontrivial normal subgroup of A_5.

c) [·/**1**] Using the fact that A_5 is simple, show that

$$[A_5, A_5] = A_5.$$

d) [·/**1**] Deduce that the derived series of A_5 is stationary and that A_5 is not solvable.

13. a) [·/**3**] Prove by induction on n that if G is a solvable group and $H \leqslant G$, then

$$\forall n \in \mathbb{N}, \quad H^{(n)} \leqslant G^{(n)}.$$

b) [·/**2**] Deduce that every subgroup of a solvable group is solvable.

14. [·/**2**] Conclude that the symmetric group S_5 is not solvable.

Remark. One can show that a polynomial $f(x)$ is *solvable by radicals*—that is, its roots can be expressed using a finite number of arithmetic operations and radicals—if and only if the symmetry group of its roots, called the *Galois group* and denoted $\mathrm{Gal}(f/K)$, is a solvable group.
In the previous questions, we showed that the symmetric group S_5 is not solvable. Now, for a general polynomial of degree 5, the symmetry group of its roots is isomorphic to S_5. Therefore, there cannot exist a general formula by radicals for the roots of a degree 5 polynomial.
More generally, for every integer $n \geqslant 5$, the symmetric group S_n is not solvable. Hence, there is no general formula by radicals to solve polynomial equations of degree strictly greater than 4.

IV — In praise of Galois

1. [·/**1000**] Deduce a general formula allowing one to solve polynomial equations of degree 5 by radicals.