Problem 1. Prove that the polynomial $P(X) = X^3 - 3X - 1$ is irreducible over $\mathbb{Q}$.

Proof. Now, if $P(X)$ is not irreducible over $\mathbb{Q}$, then clearly one of its factors must have degree 1. In other words $P(X)$ is reducible over $\mathbb{Q}$ if and only if it has a root in $\mathbb{Q}$. If possible, let $p/q \in \mathbb{Q}$ be a root of $f(X)$ where $p, q \in \mathbb{Z}$ and $(p, q) = 1$. Then we have :

$$\begin{aligned} P(p/q) = 0 &\Rightarrow p^3 - 3pq^2 - q^3 = 0 \\ &\Rightarrow p(p^2 - 3pq) = q^3, q(3pq + q^2) = p^3 \\ &\Rightarrow p|1, q|1 \end{aligned}$$

(because $(p, q) = 1$). Hence the only possible roots are ± 1. But plugging in the values we see that none of them are roots of $P(X)$. Hence $P(X)$ must be irreducible over $\mathbb{Q}$. □

Problem 2. Compute the degree $[\mathbb{Q}(\sqrt[3]{2} + \sqrt{5}) : \mathbb{Q}]$.

Proof. Let $K = \mathbb{Q}(\sqrt[3]{2} + \sqrt{5}), \alpha = \sqrt[3]{2} + \sqrt{5}$. Then note that :

$$\begin{aligned} \alpha = \sqrt[3]{2} + \sqrt{5} &\Rightarrow (\alpha - \sqrt{5})^3 = 2 \\ &\Rightarrow \sqrt{5}(3\alpha^2 + 5) = \alpha^3 + 15\alpha - 2 \\ &\Rightarrow \sqrt{5} \in K \Rightarrow \sqrt[3]{2} \in K. \end{aligned}$$

Hence we must have $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$. It is easy to see that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2, [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. We will now use the following result : E_1, E_2 be two field extensions over a field F of degree d_1, d_2 respectively where $(d_1, d_2) = 1$ and let $E = E_1E_2$, then $[E : F] = d_1d_2$. Using this result we conclude that $[K : \mathbb{Q}] = 6$. □

Problem 3. Prove that $8X^3 - 6X - 1$ is irreducible over $\mathbb{Q}$.

Proof. Let us denote the given polynomial by $f(X)$. Now, if $f(X)$ is not irreducible over $\mathbb{Q}$, then clearly one of its factors must have degree 1. In other words $f(X)$ is not irreducible over $\mathbb{Q}$ if and only if it has a root in $\mathbb{Q}$. If possible, let $p/q \in \mathbb{Q}$ be a root of $f(X)$ where $p, q \in \mathbb{Z}$ and $(p, q) = 1$. Then we have :

$$\begin{aligned} f(p/q) = 0 &\Rightarrow 8p^3 - 6pq^2 - q^3 = 0 \\ &\Rightarrow p(8p^2 - 6q^2) = q^3, q(6pq + q^2) = 8p^3 \\ &\Rightarrow p|1, q|8 \end{aligned}$$

(because $(p, q) = 1$). Hence the only possible roots are $\pm 1, \pm 1/2, \pm 1/4, \pm 1/8$. Plugging in the values we find out that none of these are roots of $f(X)$. Hence $f(X)$ must be irreducible over $\mathbb{Q}$. □

Problem 4. Let char $k = p > 0$ and $f(X) \in k[X]$ be such that $f^{'}(X) = 0$. Prove that $\exists$ a polynomial $g(X) \in k[X]$ such that $f(X) = g(X^p)$.

Proof. Let the given polynomil be $f(X) = a_nX^n + \cdots + a_1X + a_n$. Now $f^{'}(X) = 0$ means that we must have $ia_i = 0$ for $1 \leq i \leq n$. Since we are working in a field, this possible if and only if either $i = 0$ or $a_i = 0$. Hence $a_i \neq 0 \Rightarrow i = 0$ where i is treated as an element of k. But $i = 0 \Rightarrow p|i$. So the ith term in $f(X)$ has nonzero coefficient if and only if $p|i$. In particular $n = p \cdot m$. Let $g(X) = a_nX^m + a_{p(m-1)}X^{m-1} + \cdots + a_pX + a_0$. Then it is clear from the above argument that $f(X) = g(X^p)$. □

Problem 5. Let H and K be subgroups of G, $|H|^2 > |G|, |K|^2 > |G|$. Show that $H \cap K \neq \{1\}$.

Proof. We begin by proving the following result : $|HK| = |H||K|/|H \cap K|$ where $HK = \{hk | h \in H, k \in K\}$. Note that HK is just a subset of G, it need not be a subgroup. Define a map $f : H \times K \to HK$ by $(h, k) \mapsto hk$. By our definition, f is surjective. Now to prove the result we show that for any $x \in HK$ we have $|f^{-1}(x)| = |H \cap K|$. If $f(h, k) = x$ and $g \in H \cap K$ then clearly $f(hg^{-1}, gk) = x$ and so $f^{-1}(x)$ must have atleast $|H \cap K|$ elements. Conversely, if also $f(h_1, k_1) = x$ then $hk = h_1k_1 \Rightarrow h_1^{-1}h = k_1k^{-1}$. Setting $g = h_1^{-1}h \in H \cap K$ we see that $h_1 = hg^{-1}, k_1 = gk$. So $|f^{-1}(x)| = |H \cap K|$ and the result follows.

Now in our situation, let us assume that $H \cap K = \{1\} \Rightarrow |H \cap K| = 1$. Now using the above result we see that $|HK| = |H||K|$. But by our assumption about $|H|, |K|$, we have $|H||K| > |G| \Rightarrow |HK| > |G|$ and we have reached a contradiction. Hence $H \cap K \neq \{1\}$. □

Problem 6. Let $n \geq 3$. Prove that the cycle $(1\ \ 2\ \ 3)$ is not the cube of any element in S_n.

Proof. We are going to use the following facts about the permutation group S_n :

- every permutation can be written as a product of disjoint cycles;
- disjoint cycles commute;
- the order of a cycle of length m is m;
- the order of a permutation written as a product of disjoint cycles is the least common multiple of the lenghts of the cycles;
- a cycle of length $l = km$ when raised to kth power will decompose into k disjoint cycles of length m.

Now if possible assume that $(1\ \ 2\ \ 3) = \sigma^3$ for some $\sigma \in S_n$. Clearly $\sigma^9 = 1 \Rightarrow order(\sigma) = 9$. Hence if we write σ as a product of disjoint cycles, their lengths must be 3 or 9 with atleast one cycle of length 9. When we raise σ to the 3rd power, the cycles of length 3 will become trivial and each of the cycles of length 9 will decompose into 3 cycles of length 3. Clearly it is not possible that the product of more then then one disjoint 3 cycles equals just one 3 cycle. Hence $(1\ \ 2\ \ 3)$ can not be written as the cube of any element in S_n. □

Problem 7. In S_n, prove that conjugate of a cycle of length r is a cycle of length r.

Proof. We use the following fact : let $\sigma \in S_n$ and $(a_1\ \ a_2\ \ \ldots\ \ a_r)$ be a cycle in S_n, then $\sigma(a_1\ \ a_2\ \ \ldots\ \ a_r)\sigma^{-1} = (\sigma(a_1)\ \ \sigma(a_2)\ \ \ldots\ \ \sigma(a_r))$. From this it is clear that the conjugate of a cycle of length r is a cycle of length r. □

Problem 8. Determine the number of conjugacy class in S_4.

Proof. We use the following fact : the number of conjugacy classes in S_n equals the number of integer partitions of n. Hence the number of conjugacy classes in S_4 is 5. □

Problem 9. Find the number of non-isomorphic abelian groups of order 81.

Proof. For this problem we will use the structure theorem for finite abelian groups. According to which any finite abelian G can be written as $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$ where d_i's are positive integers such that $d_1|d_2|\cdots|d_r$ and are uniquely determined by the isomorphism type of G. In our situation $|G| = 81 = 3^4$, hence the cyclic subgroups occurring in the decomposition as above must have order 3 or 9 or 27 or 81. So clearly the only possibilities are :

- $\mathbb{Z}_{81}$,
- $\mathbb{Z}_3 \times \mathbb{Z}_{27}$,
- $\mathbb{Z}_9 \times \mathbb{Z}_9$,
- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9$,
- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

So there are 5 non-isomorphic abelian groups of order 81. □

Problem 10. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $1 \leq i \leq n$. Prove that $\sqrt[3]{2} \notin K$.

Proof. If possible, let us assume that $\sqrt[3]{2} \in K$. Then we must have $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]|[K : \mathbb{Q}]$. But we would show that it is not possible that $3|[K : \mathbb{Q}]$. For this we use induction on n. For $n = 1$, we have $[K : \mathbb{Q}] = 2$ and our assertion is true. So we assume that the statement is for any $n \leq N$. For $n = N + 1$ we have $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha_1, \ldots, \alpha_N)][\mathbb{Q}(\alpha_1, \ldots, \alpha_N) : \mathbb{Q}]$. Clearly $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_N)(\alpha_{N+1})$ and we have $\alpha_{N+1}^2 \in \mathbb{Q}$. Hence $1 \leq [K : \mathbb{Q}(\alpha_1, \ldots, \alpha_N)] \leq 2$ and not divisible by 3. By our induction hypothesis $[\mathbb{Q}(\alpha_1, \ldots, \alpha_N) : \mathbb{Q}]$ is also not divisible by 3. Hence by induction we have proved that $[K : \mathbb{Q}]$ is not divisible by 3. So as argued above $\sqrt[3]{2} \notin K$. □