There are “6” questions
PUT ONLY YOUR FINAL ANSWER(S) UNDER THE GIVEN QUESTION. Use the attached “scratch paper” for scratch work.

Q1: (a) 5pt) Let $\alpha$ be any solution (in $\mathbb{C}$) to the equation $x^9 - 10x^3 + 5$. What is the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$? Explain yourself.

Sol: This polynomial $p = x^9 - 10x^3 + 5$ is irreducible over $\mathbb{Q}$ by Eisenstein. Hence $p = p_\alpha$, and 

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(p_\alpha) = 9.$$ 

(b) 4pt) What is the degree of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$? Explain yourself.

Sol: We have that $x^2 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein and, as in (a), we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

(c) 10pt) What is the degree of $\mathbb{Q}(\sqrt{2}, \alpha)$ over $\mathbb{Q}$? Explain yourself.

Sol: Take $E = \mathbb{Q}(\alpha, \sqrt{2})$. We have the two expressions

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 9[E : \mathbb{Q}(\alpha)],$$

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[E : \mathbb{Q}(\sqrt{2})],$$

which imply that the degree of $E$ over $\mathbb{Q}$ is divisible by 2 and 9, and hence divisible by 18. Now, since $\sqrt{2}$ solves $x^2 - 2$ the irreducible for $\sqrt{2}$ over $\mathbb{Q}(\alpha)$ is either degree 1 (in which case $\sqrt{2} \in \mathbb{Q}(\alpha)$) or 2. Since $18 \mid [E : \mathbb{Q}]$ and $E = (\mathbb{Q}(\alpha))(\sqrt{2})$ we must have, from the above equation, that $[E : \mathbb{Q}(\alpha)] = 2$, and hence that $[E : \mathbb{Q}] = 18$.

(d) 4pt) Does 2 have a square root in $\mathbb{Q}(\alpha)$? Explain yourself.

Sol: No, if it did then we would have $[E : \mathbb{Q}(\alpha)] = 1$ and $[E : \mathbb{Q}] = 9$, which is not the case.
**Q2:** (a) 4pt) Give a concise description of the subgroup of \(\mathbb{Z}\) generated by 30, 42, and 8.

**Sol:** We have \((30, 42, 8) = \gcd(30, 42, 8)\mathbb{Z} = 2\mathbb{Z}.

(b) 10pt) Construct an explicit group isomorphism between \(\mathbb{Z}/70\mathbb{Z}\) and \(\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\). You should (a) construct a group map and (b) explain why it’s an isomorphism. (Hint: Maybe start with a map from \(\mathbb{Z}\) to \(\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\).)

**Sol:** Maps from \(\mathbb{Z}\) into any group \(G\) are specified by a choice of element \(a\). Indeed, for any choice \(a \in G\) we have a unique group map \(f_a : \mathbb{Z} \rightarrow G\) with \(f_a(1) = a\). The kernel of this map is \(\text{ord}(a)\mathbb{Z}\) and we get an induced injection \(\bar{f}_a : \mathbb{Z}/\text{ord}(a)\mathbb{Z} \rightarrow G\).

Take \(G = \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\) and \(a = (1, 1)\). Since 14 and 5 are relatively prime, \(\text{ord}(a) = 14 \cdot 5 = 70\), and we have an injective group map

\[ \bar{f}_a : \mathbb{Z}/70\mathbb{Z} \rightarrow \mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}. \]

Since the orders of these two groups are equal we find that \(\bar{f}_a\) is an isomorphism.
Q3: (7pt) Let $I = (x^2 - 5x + 2, y^3 - 1)$ in $\mathbb{C}[x, y]$. Show that the algebra map

$$f_{z_1, z_2} : \mathbb{C}[x, y] \rightarrow \mathbb{C} \text{ defined by } f_{z_1, z_2}(p(x, y)) = p(z_1, z_2),$$

for elements $z_i \in \mathbb{C}$, factors through the quotient $\mathbb{C}[x, y] \rightarrow \mathbb{C}[x, y]/I$ if and only if $z_1^2 = 5z_1 - 2$ and $z_2^3 = 1$.

**Sol:** Write $f = f_{z_1, z_2}$. If $f$ admits such a factorization then $x^2 - 5x + 2$ and $y^3 - 1$ are in the kernel of $f$, since these elements are 0 in the quotient $\mathbb{C}[x, y]/I$. This occurs if and only if

$$0 = f(x^2 - 5x + 2) = z_1^2 - 5z_1 + 2 \iff z_1^2 = 5z_1 - 2$$

and

$$0 = f(y^3 - 1) = z_2^3 - 1 \iff z_2^3 = 1.$$ 

So we see that if $f$ admits such a factorization then $z_1$ and $z_2$ solve the given equations. Conversely, if $z_1$ and $z_2$ solve the given equations then $I \subseteq \ker(f)$. In this case we (always) get the proposed factorization

$$\begin{array}{ccc}
\mathbb{C}[x, y] & \xrightarrow{f} & \mathbb{C} \\
\downarrow \text{proj} & & \downarrow \exists f \\
\mathbb{C}[x, y]/I & \xrightarrow{\bar{f}} & \\
\end{array}$$

with $\bar{f}(a + I) = f(a)$. 
Q4: (6pt) Calculate the following elements in the quaternions $\mathbb{H} = \mathbb{R} \cdot \{1, i, j, k\}$.

(a) $i^2 jk(i^{-1})$.

(b) $(1 + 3j)(4 + 2i - k)$.

(c) $(4j + 3k)^{-1}$.

Sol: (a) $i^2 jk(i^{-1}) = (-1)(-1)jkji = jkk = j$.

(b) $(1 + 3j)(4 + 2i - k) = 4 + (2 - 3)i + 12j - (6 + 1)k = 4 - i + 12j - 7k$.

(c) One check directly (by multiplying) that $(4j + 3k)^{-1} = -\frac{1}{25}(4j + 3k)$.

Q5: (6pt) Show that there does not exist a simple group of order 45.

Sol: Take $L_3$ to be the number of Sylow 3 subgroups in a given group $G$ of order $45 = 9 \cdot 5$. By Third Sylow we have

$$L_3 | 45 \quad \text{and} \quad L_3 \equiv 1 \mod 3 \quad \Rightarrow \quad L_3 \mid 5 \quad \text{and} \quad L_3 \equiv 1 \mod 3.$$ 

The only way this can happen is if $L_3 = 1$. So, there is only one Sylow 3 subgroup $P$, i.e. only one subgroup of order 9 in $G$. It follows that for any $g \in G$ the order 9 subgroup $gPg^{-1}$ must be equal to $P$. Hence $P$ is normal, and $G$ cannot simple.
Q6: (12pt) Let $p$ be a prime. Prove that $x^{(p^n - 1)} - 1$ is not irreducible over $\mathbb{F}_p$ for any $n > 1$. [Idea: Consider $\mathbb{F}_{p^n}$, and the degree $[\mathbb{F}_{p^n} : \mathbb{F}_p]$. What’s the relationship between $\mathbb{F}_{p^n}$ and $x^{(p^n - 1)} - 1$? Write $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ (can you really do this?) and consider the minimal polynomial of $\alpha$. What’s the relationship between $p_\alpha$ and $x^{(p^n - 1)} - 1$?]

Sol: You have two options here:

(Option 1) When $p$ is odd $p^n - 1$ is even, and $-1$ solves $x^{(p^n - 1)} - 1 = 0$. Hence $(x + 1)$ divides $x^{(p^n - 1)} - 1$. When $p = 2$, $-1 = 1$ still solves this equation, and we find that $(x + 1)$ divides $x^{(p^n - 1)} - 1$. In any case, $x^{(p^n - 1)} - 1$ is not irreducible.

(Option 2) Take $\alpha$ such that $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$. (Such $\alpha$ exists since $(\mathbb{F}_{p^n})^\times$ is cyclic, and we may take $\alpha$ a generator of this cyclic group.) Let $p_\alpha$ be the minimal polynomial of $\alpha$. We have

$$\deg(p_\alpha) = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$ 

Since $(\mathbb{F}_{p^n})^\times$ is cyclic of order $p^n - 1$, all nonzero elements in $\mathbb{F}_{p^n}$ solve $x^{(p^n - 1)} - 1 = 0$, by Lagrange. In particular $\alpha$ solves $x^{(p^n - 1)} - 1 = 0$, and $p_\alpha$ therefore divides $x^{(p^n - 1)} - 1$. We observe finally that

$$\deg(p_\alpha) = n < p^n - 1 = \deg(x^{(p^n - 1)} - 1)$$

to see that $x^{(p^n - 1)} - 1$ is not irreducible.