This paper contains SIX questions.
All SIX answers will be used for assessment.
Calculators, textbooks, notes and cribsheets are not permitted in this examination.
1. [3+3+3+3+3+3=18 points] Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with "T", and those which are false with "F".

a. If \( L : K \) is a finite extension of fields, then every element of \( L \) is algebraic over \( K \).

**Solution:** True (if \( [L : K] < \infty \) and \( \alpha \in L \) then \( [K(\alpha) : K] < \infty \) and hence \( \alpha \) is algebraic).

b. If \( L : K \) is a field extension and \( L = K(\alpha) \), then for any \( \beta \in L \) there exist \( a, b \in K \) with \( \beta = a + b\alpha \).

**Solution:** False (consider \( L = \mathbb{Q}(2^{1/3}) \) and \( 2^{2/3} \in L \), and observe that there exist no \( a, b \in \mathbb{Q} \) for which \( 2^{2/3} = a + b2^{1/3} \)).

c. There is a homomorphism of finite fields \( \varphi : \mathbb{F}_7 \to \mathbb{F}_{97} \).

**Solution:** False (if true, then since \( \varphi(1) = 1 \), we would have \( 0 = \varphi(1+1+1+1+1+1+1) = \varphi(1) + \ldots + \varphi(1) = 7 \in \mathbb{F}_{97} \), leading to a contradiction).

d. If \( L : K \) is a field extension, and \( \alpha \) and \( \beta \) are distinct elements of \( L \) having the same minimal polynomial over \( K \), then \( K(\alpha) \) and \( K(\beta) \) are isomorphic fields.

**Solution:** True (this is an immediate consequence of Theorem 3.2 from the course).

e. Let \( K \) be a field of characteristic \( p \). Suppose that \( L : K \) is a field extension and \( \tau \in L \). If \( \tau^p \) is transcendental over \( K \), then \( \tau \) is transcendental over \( K \).

**Solution:** True (if \( \tau \) were algebraic over \( K \), then one would have \( [K(\tau) : K] < \infty \). But \( K(\tau^p) \subseteq K(\tau) \), and so \( [K(\tau^p) : K] < \infty \), whence \( \tau^p \) is algebraic, yielding a contradiction).

f. The polynomial \( x^5 + x^4 + x^3 + x^2 + x + 1 \) is irreducible over \( \mathbb{Q} \).

**Solution:** False (one has the factorisation \( x^5 + x^4 + x^3 + x^2 + x + 1 = (x+1)(x^4 + x^2 + 1) \)).

2. [3+3+3+3=12 points]

(a) Suppose that \( L : K \) is a field extension. Define what is meant by the *degree* of \( L : K \).

**Solution:** The *degree* of \( L : K \) is the dimension of \( L \) as a vector space over \( K \).

(b) Suppose that \( L : K \) is a field extension with \( K \subseteq L \), and \( \alpha \in L \) is algebraic over \( K \). Define what is meant by the *minimal polynomial* of \( \alpha \) over \( K \).

**Solution:** The *minimal polynomial* of \( \alpha \) over \( K \) is the unique monic polynomial \( m_\alpha(K) \) having the property that \( \ker(E_\alpha) = (m_\alpha(K)) \), where \( E_\alpha : K[t] \to L \) denotes the evaluation map defined by putting \( E_\alpha(f) = f(\alpha) \).

(c) For \( i = 1 \) and \( 2 \), let \( L_i : K_i \) be a field extension relative to the embedding \( \varphi_i : K_i \to L_i \). Suppose that \( \sigma : K_1 \to K_2 \) and \( \tau : L_1 \to L_2 \) are isomorphisms. Define what is meant by the statement that \( \tau \) *extends* \( \sigma \).

**Solution:** The isomorphism \( \tau \) *extends* \( \sigma \) if \( \tau \circ \varphi_1 = \varphi_2 \circ \sigma \).

(d) Let \( L : K \) be a field extension relative to the embedding \( \varphi : K \to L \), and let \( M \) be a subfield of \( L \) containing \( \varphi(K) \). Define what is meant by the statement that \( \sigma : M \to L \) is a *\( K \)-homomorphism*.

**Solution:** The mapping \( \sigma : M \to L \) is a *\( K \)-homomorphism* when \( \sigma \) leaves \( \varphi(K) \) pointwise fixed, so that, for all \( \alpha \in \varphi(K) \), one has \( \sigma(\alpha) = \alpha \).

*Continued*...
3. [8+5+6+6=25 points] Let \( \theta \) denote the real number \( \sqrt[4]{2} + \sqrt[4]{2} \).

(a) Calculate the minimal polynomial of \( \theta \) over \( \mathbb{Q} \).

**Solution:** One has \( \theta^4 - 2 = \sqrt[4]{2} \), whence \( (\theta^4 - 2)^2 - 2 = 0 \). We therefore deduce that the polynomial \( f(t) = t^6 - 4t^3 + 2 \) has \( \theta \) as a root, whence the minimal polynomial of \( \theta \) over \( \mathbb{Q} \) divides \( f(t) \). The polynomial \( f(t) \) is monic, has all of its coefficients save the leading one divisible by 2, and has constant coefficient not divisible by 4. Hence, by Eisenstein’s criterion and Gauss’ Lemma, it follows that \( f(t) \) is irreducible over \( \mathbb{Q} \), and hence is the minimal polynomial of \( \theta \) over \( \mathbb{Q} \).

(b) What is the degree of the field extension \( [\mathbb{Q}(\theta) : \mathbb{Q}] \)? Justify your answer.

**Solution:** One has \( [\mathbb{Q}(\theta) : \mathbb{Q}] = \deg(m_\theta(\mathbb{Q})) = \deg(t^6 - 4t^3 + 2) = 6 \).

(c) Does there exist a subfield \( K \) of the field \( \mathbb{Q}(\theta) \) having the property that \([K : \mathbb{Q}] = 5\)? Justify your answer.

**Solution:** Suppose that there exists a subfield \( K \) of \( \mathbb{Q}(\theta) \) with \([K : \mathbb{Q}] = 5\). Then, by the tower law, one has \( 6 = [\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q}(\theta) : K][K : \mathbb{Q}] = 5[\mathbb{Q}(\theta) : K] \). Since 5 does not divide 6, we obtain a contradiction. So there exists no subfield \( K \) of \( \mathbb{Q}(\theta) \) with \([K : \mathbb{Q}] = 5\).

(d) Is the real number \( \theta \) constructible by ruler and compass? Justify your answer.

**Solution:** If \( \theta \) were to be constructible by ruler and compass, one would have \([\mathbb{Q}(\theta) : \mathbb{Q}] = 2^r \) for some non-negative integer \( r \). Then, using our solution of part (b) we would have \( 6 = [\mathbb{Q}(\theta) : \mathbb{Q}] = 2^r \), leading to a contradiction, since 3 divides the left hand side here but not the right. Thus \( \theta \) is not constructible by ruler and compass.

4. [15 points] Let \( L : K \) be a field extension. Suppose that \( \alpha \in L \) is algebraic over \( K \) and \( \beta \in L \) is transcendent over \( K \). Suppose also that \( \alpha \notin K \). Show that \( K(\alpha, \beta) : K \) is not a simple field extension.

**Solution:** Suppose that \( K(\alpha, \beta) = K(\gamma) \) for some \( \gamma \in L \). Since \( \beta \in K(\gamma) \) is transcendent over \( K \), the field extension \( K(\gamma) : K \) is not algebraic, and hence \( \gamma \) is transcendent over \( K \). Since \( \alpha \in K(\gamma) \), we have \( \alpha = f(\gamma)/g(\gamma) \) for some \( f, g \in K[t] \) with \( g \neq 0 \). Thus \( \gamma \) is a root of \( h = \alpha g - f \in K(\alpha)[t] \). Since \( \alpha \notin K \) and \( g \neq 0 \), the polynomial \( h \) cannot be the zero polynomial, and therefore \( \gamma \) is algebraic over \( K(\alpha) \). But then, since \( \alpha \) is algebraic over \( K \), this implies that \( [K(\gamma) : K] = [K(\gamma) : K(\alpha)] [K(\alpha) : K] < \infty \), contradicting the transcendency of \( \gamma \). So \( K(\alpha, \beta) : K \) cannot be a simple extension.

5. [6+9=15 points] Suppose that \( K \subseteq L \) are fields.

(a) Show that when \( 1 < [L : K] < \infty \), then there exists \( \beta \in L \) for which

\[ [L : K(\beta)] < [L : K]. \]

**Solution:** The hypothesis \([L : K] > 1\) ensures that there exists an element \( \beta \in L \setminus K \). But then if \([K(\beta) : K] = d\), we have \( d \geq 2 \). Thus, by the tower law, one finds that \([L : K] = [L : K(\beta)][K(\beta) : K] = d[L : K(\beta)]\), whence \([L : K(\beta)] = [L : K]/d \leq [L : K]/2 < [L : K]\).
(b) Suppose that $[L : K] < \infty$. Show that there exist elements $\alpha_1, \ldots, \alpha_n \in L$ for which $L = K(\alpha_1, \ldots, \alpha_n)$.

**Solution:** If $L = K$ then we are done. We proceed by induction on $[L : K]$, with the trivial case $L = K$ as the basis. Suppose that the desired conclusion holds whenever $[L : K] < N$, and consider the situation with $[L : K] = N > 1$. From part (a), there exists $\alpha_1 \in L$ with $[L : K(\alpha_1)] < N$. But then the inductive hypothesis ensures that there exist $\alpha_2, \ldots, \alpha_n \in L$ for which $L = K(\alpha_1)(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$, confirming the inductive step.

6. [5+5+5=15 points] Suppose that $L$ is a subfield of $\mathbb{C}$ having the property that $L : \mathbb{Q}$ is algebraic, and every non-constant polynomial in $\mathbb{Q}[t]$ has all of its roots lying in $L$.

   (a) Suppose that $\varphi$ is an automorphism of $\mathbb{C}$. Show that $\varphi$ fixes $\mathbb{Q}$ pointwise.

**Solution:** Since $\varphi(1) = 1$ (and $\varphi$ is a homomorphism), one has $\varphi(n) = \varphi(1 + \ldots + 1) = \varphi(1) + \ldots + \varphi(1) = n$ for each $n \in \mathbb{N}$. Thus, the homomorphism properties of $\varphi$ ensure that $\varphi(0) = 0$, $\varphi(-n) = -n$ for $n \in \mathbb{N}$, and $\varphi(a/b) = a/b$ for each $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Thus $\varphi$ fixes $\mathbb{Q}$ pointwise.

   (b) Suppose as in (a) that $\varphi$ is an automorphism of $\mathbb{C}$. Show that whenever $\alpha \in L$, then $\varphi(\alpha) \in L$.

**Solution:** Given $\alpha \in L$, one has that $\alpha$ is algebraic, and so the minimal polynomial $m_\alpha(\mathbb{Q})$ exists with all of its coefficients lying in $\mathbb{Q}$. In addition, one has $\varphi(m_\alpha(\mathbb{Q})) = m_\alpha(\mathbb{Q})$, so $\varphi(\alpha)$ is another root of $m_\alpha(\mathbb{Q})$. We may assume that all the roots of $m_\alpha(\mathbb{Q})$ lie in $L$ (from the opening hypothesis of the problem), and so $\varphi(\alpha) \in L$.

   (c) Show that when $\varphi$ is an automorphism of $\mathbb{C}$, one has $\varphi(L) = L$.

**Solution:** It follows from part (b) that when $\alpha \in L$, then $\varphi(\alpha) \in L$, and hence $\varphi(L) \subseteq L$. Next, consider $\alpha \in L$, and put $\beta = \varphi^{-1}(\alpha)$. Since $\varphi^{-1}$ is an automorphism of $\mathbb{C}$, one sees that $\varphi^{-1}(m_\alpha(\mathbb{Q})) = m_\alpha(\mathbb{Q})$. Thus $\beta$ is a root of $m_\alpha(\mathbb{Q})$, and so $\beta$ lies in $L$. But then we have $\alpha = \varphi(\beta) \in \varphi(L)$. We have therefore shown that $L \subseteq \varphi(L)$. In combination with our earlier conclusion, we now have $L \subseteq \varphi(L) \subseteq L$, whence $L = \varphi(L)$, as desired.

*End of examination.*