MATH 220C: PROBLEM SHEET
APRIL 3, 2018

You may find it helpful to attempt the following problems.

(1) Show that if N is large enough, then $x^5 - Nx + 1$ is irreducible over $\mathbf{Q}$. (Hint: First (using Rouché's theorem, or some other method) show that four of the roots in $\mathbf{C}$ are absolutely greater that 1.)

(2) If C is a distinguished class of extensions, and $N \supset L \supset K$, $N \supset M \supset K$ are two towers with L/K, M/K in C, then prove that ML/K lies in C.

(3) An extension with $[L : K] < \infty$ is said to be *finite*. Prove that the class of finite extensions is distinguished.

(4) Let L/K be an extension and suppose that $\alpha \in L$. If α is algebraic, let f denote the minimal polynomial of α over K.

(i) Prove that if α is algebraic, then $[K(\alpha) : K]$ is equal to the degree of f. (Remark: An extension L/K in which every element of L is algebraic over K is termed *algebraic*: otherwise it is termed *transcendental*.)

(ii) Prove that a finite extension is algebraic.

(iii) Prove that if L/K is an extension, then the set of elements of L algebraic over K forms a field.

(iv) Give an example of an algebraic extension which is not finite.

(v) Prove that the class of algebraic extensions is distinguished.

(5) If α is algebraic over K, consider the endomorphism $T(\beta) = \alpha\beta$ of the K-vector space $K(\alpha)$. Show that the determinant of $xI - T$ (where I = identity) is the minimal polynomial of α over K.

(6) Find a splitting field over $\mathbf{Q}$ for each of the following polynomials, and in each case, calculate the degree over $\mathbf{Q}$ of the field:

$x^4 - 5x^2 + 6$, $x^4 + 5x^2 + 6$, $x^6 - 1$, $x^6 + 1$, $x^p - 1$, $x^p - q$ (p, q primes).

(7) Show that if K/k is an algebraic extension, and P is the set of elements of K which are purely inseparable over k, then P is a field.

(8) Show that the class of purely inseparable extensions is distinguished.

(9) (a) Let K/k be a finite extension. Show that there is an intermediate field L such that L/k is separable and K/L is purely inseparable. [Hint: Let L be the set of elements of K separable over k. Consider any $\alpha \in K$ with minimal ploynomial f over k. Let n be such that $f \in k[x^{p^n}]$ but $f \notin k[x^{p^{n+1}}]$. Deduce that α^{p^n} is separable over k. Conclude.]

(b) Show that the field L above is unique.

(c) Define $[K : k]_s = [L : k]$ and $[K : k]_i = [K : L]$. Show that $[- : -]_s$ and $[- : -]_i$ satisfy tower laws. [Hint: You can slog this out. Alternatively, prove that $[K : k]_s =$ the number of distinct k-embeddings of K in L, and conclude.]

(10) Suppose that K/k is algebraic and Char(k)$= p > 0$. Let $K^p = \{\alpha^p : \alpha \in K\}$.

(a) Show that K^p is a field.

(b) By considering the minimal polynomial of α over $K(\alpha^p)$, show that if K/k is separable, then $K = k(K^p)$.

(c) Suppose that K/k is finite and $K = k(K^p)$. Show that if $\alpha_1, ..., \alpha_n$ are k-linearly independent, then so are $\alpha_1^p, ..., \alpha_n^p$. [Hint: Extend to a basis and take p-th powers.].

(d) Suppose that K/k is finite and $K = k(K^p)$. Suppose that $\alpha \in K$ is inseparable over k, and so has minimal polynomial of the form $a_0 + a_1 x^p + ... + a_r x^{p^r}$. Show that $1, \alpha, ..., \alpha^r$ are dependent over k, and obtain a contradiction. Deduce that K/k is separable.

(11) Suppose that K/k is finite. Prove that K/k is simple if and only if there are only finitely many fields F intermediate between K and k. [Hints: (i) Assume that $K = k(\alpha)$ and that α has minimal polynomial f over F. Show that F is generated over k by the coefficients of f. Deduce that there are only finitely many F.

(ii) Suppose that K/k is not simple. We may assume that k is infinite (why?). Show that $k(x, y)/k$ is not simple for some x, y: hence show that the fields $k(x + cy)$ as c varies in k are all distinct.]

(12) Determine the Galois groups of the following polynomials:

(a) $x^3 - x - 1$ over $\mathbf{Q}$.

(b) $x^3 - 10$ over $\mathbf{Q}$.
(c) $x^3 - 10$ over $\mathbf{Q}(\sqrt{2})$.
(d) $x^3 - 10$ over $\mathbf{Q}(\sqrt{-3})$.
(e) $x^3 - x - 1$ over $\mathbf{Q}(\sqrt{-23})$.
(f) $x^4 - 5$ over $\mathbf{Q}$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{-5})$.
(g) $x^4 - a$ over $\mathbf{Q}$, where a is any squarefree integer $\neq 0, \pm 1$.
(h) $x^4 + 2$ over $\mathbf{Q}(i)$.
(i) $(x^2 - 2)(x^2 - 3)(x^2 - 5)$ over $\mathbf{Q}$.
(j) $(x^2 - p_1)...(x^2 - p_n)$ over $\mathbf{Q}$, where $p_1, ..., p_n$ are distinct primes.
(k) $x^n - t$ over $\mathbf{C}(t)$, where t is transcendental over $\mathbf{C}$.

(13) (a) Suppose that $[K : k] = 2$, that every element of K has a square root in K, that every polynomial of odd degree in $k[x]$ has a root in k, and that $\mathrm{char}(k) \neq 2$. Prove that K is algebraically closed.

[Hint: Let f be an irreducible polynomial over k, with splitting field L over k and Galois group G, with $H = Gal(L/K)$. By considering the fixed field of a Sylow 2-subgroup of G, show that $|G| = 2^n$, $|H| = 2^{n-1}$ for some n. By further considering the fixed field of a subgroup of index 2 in H, show that if $|H| > 1$, then there is an irreducible polynomial of degree 2 over K.]

(b) Prove that $\mathbf{C}$ is algebraically closed.

(14) Let a, b, c be elements of a field k of characteristic $\neq 2$ or 3, such that $f(X) = X^3 + aX^2 + bX + c$ is irreducible over k, and let x_1, x_2, x_3 be the roots of $f(X)$ in a splitting field.

(i) If $\Delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$, show that $\Delta^2 \in k$, and obtain a formula for Δ^2 in terms of a, b, c.

(ii) If $\omega \neq 1$ is a cube root of 1 in k, show that $(x_1 + \omega x_2 + \omega^2 x_3)^3$ is in $k(\Delta)$, and obtain a formula for it in terms of a, b, c and Δ.

(15) Suppose that t is transcendental over a field K. Show that there exists a unique K-automorphism σ of $K(t)$ such that $\sigma(t) = 1/(1 - t)$.

Prove that σ^3 is equal to the identity. Find $\mathrm{Fix}(< \sigma >)$, and show that it is a simple transcendental extension of K.

If the characteristic of K is not equal to 2, show that there exists a unique K-automorphism τ of $K(t)$ such that $\tau(t) = 2t$. Prove that $\mathrm{Fix}(<\tau>) = K$ if and only if K is of characteristic zero.

(16) Suppose that k is a field of characteristic $p > 0$, and that x, y are independent transcendentals over k (that is, if $f \in k[X, Y]$ and $f(x, y) = 0$, then $f = 0$)). Let $K = k(x, y)$ and $L = k(x^p, y^p)$. Prove that $[K : L] = p^2$, but that if z lies in K, then z^p lies in L, and so $K \neq L(z)$.

Show further that there are infinitely many fields between L and K.

(17) Comment on the following "proof" of the existence of an algebraic closure:

"Let k be a field, and S the set of all fields which are algebraic over k, ordered under inclusion. Then S is non-empty, and if T is a subset of S such that $K, L \in T$ implies that $K \subset L$ or $L \subset K$, then $\cup_{H \in T} H$ is an element of S and an upper bound for T. Hence, by Zorn's Lemma, there is a maximal element $M \in S$. If M is not algebraically closed, then we can construct an algebraic extension of M, and this contradicts the maximality of M. Hence M is an algebraic closure of k."

[Hint: It IS wrong!]

(18) Let G be a (possibly infinite) group, let K be a normal subgroup of finite index in G, and let $t_1, ..., t_r$ be representatives of the cosets of K in G. Suppose that V is a finite dimensional, completely reducible $\mathbf{C}G$-module. Show that:

(a) If U is a $\mathbf{C}K$-submodule of V, and $g \in G$, then $Ug = \{ug | u \in U\}$ is a $\mathbf{C}K$-submodule of V.

(b) If U is a $\mathbf{C}K$-submodule of V, then $\sum_1^r Ut_i$ is a $\mathbf{C}G$-submodule of V.

(c) V is completely reducible when regarded as a $\mathbf{C}K$-module.

(19) A (not necessarily finite) group G has a (normal) subgroup H of index 2, and t is an element of G but not H. A $\mathbf{C}G$-space V is given. Show that if ϕ is a $\mathbf{C}H$ endomorphism of V, then the map $\phi^t : V \to V$ given by $\phi^t(v) = t^{-1}\phi(tv)$ $(v \in V)$ is also a $\mathbf{C}H$-endomorphism.

By considering $(1/2)(\phi + \phi^t)$ for suitably chosen ϕ, prove that if V is completely reducible as a $\mathbf{C}H$-space, it is also completely reducible as a $\mathbf{C}G$-space.

(20) (i) A representation of a group G is said to be *faithful* if it has trivial kernel. Show that a finite group which has a faithful irreducible complex representation must have a cyclic centre. [Hint: Schur's lemma.]

(ii) A group G of order 18 has a non-cyclic abelian subgroup A of order 9, and an element x of order 2 such that $x^{-1}ax = a^{-1}$ for all $a \in A$. By considering the action of A on an irreducible $\mathbf{C}G$-module, prove that G has no faithful irreducible complex representation.

(21) (i) Let p be a prime number, and let G be a finite p-group with cyclic centre Z. Suppose that ρ is a faithful representation over $\mathbf{C}$ of G. Prove that some irreducible component of ρ is faithful. [Hint: You may find it helpful to use the facts that, since G is a p-group, Z is non-trivial, and any non-trivial normal subgroup of G intersects G non-trivially.]

(ii) Deduce that a finite p-group has a faithful irreducible representation over $\mathbf{C}$ if, and only if, its centre is cyclic.

(22) (a) Suppose that y is an element of order 3 in a finite group G, and that y is conjugate to y^{-1}. Show that if χ is any $\mathbf{C}$-valued character of G, then $\chi(y)$ is a rational integer, and $\chi(y) \equiv \chi(1)$ modulo 3.

(b) Suppose further that 1, y, y^{-1} are the only elements of G which commute with y. Show that G has precisely 3 irreducible complex-valued characters of degree coprime to 3.

(23) (a) Let G be a finite group. Suppose that y is an element of G of order 4 which is conjugate to its inverse in G. Prove that if χ is a character of G, then $\chi(y)$ is an integer, and $\chi(y) \equiv \chi(1)$ modulo 2.

(b) Prove that if 1, y, y^2, and y^3 are the only elements of G which commute with y, then G has precisely 4 irreducible characters of odd degree. [Hint: Orthogonality relations for the character table.]

(24) A group of order 720 has 11 conjugacy classes. Two representations of the group are known, and have corresponding characters α and β. The table below gives the sizes

of the classes and the values which α and β take on them:

	1	15	40	90	45	120	144	120	90	15	40
α	6	2	0	0	2	2	1	1	0	-2	3
β	21	1	-3	-1	1	1	1	0	-1	-3	0

Prove that the group has an irreducible representation of degree 16, and write down the values that the corresponding character has on the classes.