MA3D5

1. (a) Define the elementary symmetric polynomials σ_i in variables $\alpha_1, \ldots, \alpha_n$. **[3]**

(b) Let $P \in \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$. Define what it means that P is symmetric. Now assume P to be symmetric. Prove that P can be expressed as a polynomial over $\mathbb{Z}$ in the elementary symmetric polynomials $\sigma_i = \sigma_i(\alpha_1, \ldots, \alpha_n)$. **[9]**

(c) Let $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, $\alpha + \beta + \gamma + \delta = 0$. Put **[4]**

$$\begin{aligned} x &= (\alpha + \beta)(\gamma + \delta), \\ y &= (\alpha + \gamma)(\beta + \delta), \\ z &= (\alpha + \delta)(\beta + \gamma). \end{aligned}$$

Let σ_i denote the elementary symmetric polynomials in $\alpha, \beta, \gamma, \delta$ and τ_i those in x, y, z. Prove that for every $i \geq 0$ there exists a polynomial $p_i \in \mathbb{C}[u_2, u_3, u_4]$ such that $\tau_i = p_i[\sigma_2, \sigma_3, \sigma_4]$.

(d) Deduce from (c) that every degree 4 equation can be solved by radicals. You may assume that every degree 3 equation can. **[6]**

(e) Compute p_1 explicitly. **[3]**

SOLUTION.

(a) $\sigma_i(\alpha_1, \ldots, \alpha_n)$ is the sum of the elements of

$$\{\alpha_{k_1} \cdots \alpha_{k_i} \mid 1 \leq k_1 < \cdots < k_i \leq n\}.$$

(b) Symmetric means invariant under any permutation of the variables $\alpha_1, \ldots, \alpha_n$.

Required proof. A polynomial is a linear combination of monomials $\alpha^{\underline{b}}$. Define the lex order on the set of monomials as follows. Write a monomial as

$$(\alpha_1 \cdots \alpha_1)(\alpha_2 \cdots \alpha_2) \cdots (\alpha_n \cdots \alpha_n)1$$

where 1 is an end-of-word marker. Then a word beats another if and only if it beats it the first time they differ where $1 < \alpha_1 < \alpha_2 < \cdots$. The *leading term* of P is its first term in lex order. The leading term is a constant times $\alpha^{\underline{b}}$ where $b_1 \geq b_2 \geq \cdots \geq b_n$.

Consider the polynomial $Q = \sigma_1^{c_1} \cdots \sigma_n^{c_n}$. Its leading term is the product of the leading terms in the factors which is

$$\alpha_1^{c_1+c_2+\cdots+c_n} \alpha^{c_2+\cdots+c_n} \cdots \alpha^{c_n}.$$

We hit the leading term of P by choosing $c_i = b_i - b_{i+1}$ which is ≥ 0 as required. Then P minus a scalar multiple of Q has a smaller leading term than P has. Finish with induction.

(c) The set $\{x, y, z\}$ is symmetric in the $\alpha, \beta, \gamma, \delta$. So τ_i is a polynomial in all σ_i with $i \geq 1$ by (b). But $\sigma_2, \sigma_3, \sigma_4$ are the only ones needed: $\sigma_1 = 0$ by assumption and $\sigma_i = 0$ for $i \geq 5$ because $\#\{\alpha, \beta, \gamma, \delta\} = 4$.

(d) One can obtain x, y, z by radicals by (c) and because cubics can be done. One can obtain $\alpha+\beta$ because it is a square root of $-x$; similarly for $\alpha+\gamma$ and $\alpha+\delta$. Now

$$\alpha = \frac{(\alpha+\beta+\gamma+\delta)+2\alpha}{2} = \frac{(\alpha+\beta)+(\alpha+\gamma)+(\alpha+\delta)}{2}$$

and likewise for β, γ, δ.

(e) $\tau_1 = x+y+z = (\alpha+\beta)(\gamma+\delta)+(\alpha+\gamma)(\beta+\delta)+(\alpha+\delta)(\beta+\gamma)$
$= 2(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta) = 2\sigma_2$.

STATUS. Variation on bookwork. Part (e) is quite different from what we did.

2. (a) (i) Let $K \subset L$ be a field extension. Define $[L:K]$. **[2]**

(ii) Let $K \subset L$ and $L \subset M$ be two finite field extensions. Prove that $K \subset M$ is finite, and $[M:K] = [M:L][L:K]$. **[5]**

(iii) Let $\alpha = \sqrt[5]{2} \in \mathbb{R}$. Prove $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$. **[4]**

(iv) Let $\beta = \alpha + \alpha^3$. Use the statement of (ii) to prove $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. **[5]**

(b) Define $\alpha = \exp(2\pi i/3) \in \mathbb{C}$. Let $\mathbb{C}(u)$ denote the field of rational functions in a variable u. Define the $\mathbb{C}$-automorphisms s, t of $\mathbb{C}(u)$ by

$$s(u) = u^{-1}, \qquad t(u) = \alpha\, u^{-1}$$

(and s, t fix every element of $\mathbb{C}$). Put $G = \langle s, t\rangle$.

(i) Without proof define an isomorphism $\phi\colon G \to S_3$ to the symmetric group, for example by giving $\phi(s)$ and $\phi(t)$. **[3]**

(ii) Without proof list all subgroups $H \subset G$ (for example by giving generators for them) and for each of them a function $f \in \mathbb{C}(u)$ such that $\mathbb{C}(u)^H = \mathbb{C}(f)$. **[6]**

SOLUTION.

(a) (i) L is a vector space over K; addition in the vector space comes from addition in the field; scalar multiplication in L comes from multiplication in L. Now $[L:K]$ is the dimension of this vector space.

(ii) Let $\{x_i\}_i$ be an L-basis of M, and $\{y_j\}_j$ a K-basis of L. We claim that $\{x_i y_j\}_{ij}$ is a K-basis for M.

Spanning. Let $u \in M$. Since x_i span M over L we can write $u = \sum_i a_i x_i$ with $a_i \in L$. Since y_j span L over K we can write $a_i = \sum_j b_{ij} y_j$. Then $u = \sum_i a_i x_i = \sum_i (\sum_j b_{ij} y_j) x_i = \sum_{ij} b_{ij} x_i y_j$. This proves spanning.

Independence. Suppose $\sum_{ij} b_{ij} x_i y_j = 0$ with $b_{ij} \in K$. This says that some L-linear combination of the y_j is zero. But the y_j are L-independent so the coefficients are zero, that is, $\sum_i b_{ij} x_i = 0$ for all j. Now the x_i are K-independent so $b_{ij} = 0$ for all i, j. This proves independence.

(iii) The polynomial $f = x^5 - 2 \in \mathbb{Z}[x]$ is Eisenstein for 2. So it is irreducible. But α is a root of f. So $[\mathbb{Q}(\alpha):\mathbb{Q}] = \deg(f) = 5$.

(iv) Clearly $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$. By the Tower Law we have $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = 5$. So $[\mathbb{Q}(\beta) : \mathbb{Q}]$ is a divisor of 5, that is, it is 1 or 5. But it can't be 1 because otherwise $\beta \in \mathbb{Q}$ so α would be a zero of a degree 3 polynomial $x^3 + x - \beta$, contradicting $\deg(\alpha) = 5$. So $[\mathbb{Q}(\beta) : \mathbb{Q}] = 5$ and $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$

(b) (i) $\phi(s) = (12)$, $\phi(t) = (23)$.

(ii)

subgroup	1	$\langle s \rangle$	$\langle t \rangle$	$\langle sts \rangle$	$\langle st \rangle$	G
f	u	$u + u^{-1}$	$u + \alpha\, u^{-1}$	$u + \alpha^2 u^{-1}$	u^3	$u^3 + u^{-3}$

STATUS. (a)(i) and (a)(ii) are bookwork. (a)(iii) and (a)(iv) are unseen but in the same vein as many examples and sheet exercises. (b) is an easier version of a sheet exercise.

3. (a) Let L be a field, $G \subset \mathrm{Aut}(L)$ a subgroup and $K = L^G$. Suppose that the G-orbit $G\alpha := \{g\alpha \mid g \in G\}$ is finite for every $\alpha \in L$. Prove that L/K is algebraic, normal and separable. [Hint. Mimic our proof of the situation where G is finite.] **[7]**

(b) Let $\varepsilon = \exp(2\pi i/7) \in \mathbb{C}$. You may use the fact that ε has degree 6 over $\mathbb{Q}$. We put

$$\alpha = \varepsilon + \varepsilon^6, \quad \beta = \varepsilon^2 + \varepsilon^5, \quad \gamma = \varepsilon^3 + \varepsilon^4.$$

(i) Prove $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\varepsilon)$ and $[\mathbb{Q}(\varepsilon) : \mathbb{Q}(\alpha)] \in \{1, 2\}$ and use the Tower Law to deduce that α is of degree 3 or 6 over $\mathbb{Q}$. **[4]**

(ii) Compute the polynomial $f = (x - \alpha)(x - \beta)(x - \gamma)$ explicitly and hence prove that it is in $\mathbb{Z}[x]$. **[5]**

(iii) Prove that α is of degree 3 over $\mathbb{Q}$. **[2]**

(iv) Find explicitly an $r \in \mathbb{Z}[x]$ such that $r(\alpha) = \beta$. **[3]**

(v) Prove that $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$. You may use theorems from the course but you should formulate them if you do. **[4]**

SOLUTION.

(a) Let $\alpha \in L$. We will be done if we can prove that α is algebraic over K, and its minimum polynomial g over K factors into distinct linear factors over L.

Let $\{g\alpha \mid g \in G\} = \{\alpha_1, \ldots, \alpha_n\}$ be the G-orbit of α (it is given that it is finite), and assume $\alpha_i \neq \alpha_j$ whenever $i \neq j$. Then $f := \prod_{i=1}^n (x - \alpha_i)$ is clearly invariant under G, that is, $f \in K[x]$. Now $f(\alpha) = 0$ so α is algebraic over K. Also, g is a divisor of f by definition of minimum polynomial. So g factors into distinct linear factors of L as required.

(b) (i) Since $\alpha = \varepsilon + \varepsilon^6$ we have $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\varepsilon)$. We have $\varepsilon^2 - \alpha\,\varepsilon + 1 = 0$ so $d := [\mathbb{Q}(\varepsilon) : \mathbb{Q}(\alpha)] \in \{1, 2\}$. By the Tower Law we find $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\varepsilon) : \mathbb{Q}]/d = 6/d \in \{3, 6\}$.

(ii) Using the fact that $1+\varepsilon+\varepsilon^2+\cdots+\varepsilon^6=0$ we find:

$$\begin{aligned}
&\alpha+\beta+\gamma=\varepsilon^1+\cdots+\varepsilon^6=-1,\\
&\alpha\beta+\alpha\gamma+\beta\gamma=\\
&\qquad=(\varepsilon^3+\varepsilon^6+\varepsilon^8+\varepsilon^{11})+(\varepsilon^4+\varepsilon^5+\varepsilon^9+\varepsilon^{10})+(\varepsilon^5+\varepsilon^6+\varepsilon^8+\varepsilon^9)\\
&\qquad=(\varepsilon^3+\varepsilon^6+\varepsilon^1+\varepsilon^4)+(\varepsilon^4+\varepsilon^5+\varepsilon^2+\varepsilon^3)+(\varepsilon^5+\varepsilon^6+\varepsilon^1+\varepsilon^2)\\
&\qquad=2(\varepsilon^1+\cdots+\varepsilon^6)=-2,\\
&\alpha\beta\gamma=(\varepsilon^3+\varepsilon^6+\varepsilon^1+\varepsilon^4)(\varepsilon^3+\varepsilon^4)\\
&\qquad=(\varepsilon^6+\varepsilon^9+\varepsilon^4+\varepsilon^7)+(\varepsilon^7+\varepsilon^{10}+\varepsilon^5+\varepsilon^8)\\
&\qquad=(\varepsilon^6+\varepsilon^2+\varepsilon^4+\varepsilon^0)+(\varepsilon^0+\varepsilon^3+\varepsilon^5+\varepsilon^1)=1+(\varepsilon^0+\cdots+\varepsilon^6)=1
\end{aligned}$$

so $f=x^3+x^2-2\,x-1$.

(iii) The degree of α over $\mathbb{Q}$ is at most 3 by (ii) so it must be 3 by (i).

(iv) We have $\alpha=\varepsilon+\varepsilon^{-1}$ and $\beta=\varepsilon^2+\varepsilon^{-2}$ so $\beta=\alpha^2-2$.

(v) A theorem from the course says splitting fields are always finite and normal. Another theorem says finite, normal, separable implies Galois. Clearly, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is separable (because the characteristic is zero) so it remains to prove that it is a splitting field.

By (iv) we have $\beta\in\mathbb{Q}(\alpha)$. Also $\gamma\in\mathbb{Q}(\alpha)$ because $\alpha\beta\gamma=1$. Since $f=(x-\alpha)(x-\beta)(x-\gamma)\in\mathbb{Q}[x]$ by (ii) it follows that $\mathbb{Q}(\alpha)$ is a splitting field of f.

STATUS. (a) is a variation on bookwork. (b) is unseen but in the same vein as many examples and sheet exercises.

4. Let $K\subset L$ be a finite field extension.

(a) Define the Galois group $G=\mathrm{Gal}(L/K)$. **[2]**

(b) Let $\sigma\colon K\to M$ be a field homomorphism. Prove that the number of K-homomorphisms $L\to M$ is at most $[L:K]$. **[8]**

(c) Prove $\#G\le[L:K]$ and state without proof when equality holds. **[4]**

(d) For a subset $H\subset G$ we define $H^\dagger=L^H=\{x\in L\mid hx=x \text{ for all } h\in H\}$. Prove that $H^\dagger$ is a subfield of L. Prove $H_1\subset H_2\Rightarrow H_1^\dagger\supset H_2^\dagger$. **[4]**

(e) Let $\alpha=\sqrt[4]{5}\in\mathbb{R}$, $K=\mathbb{Q}(i)\subset\mathbb{C}$ and $L=\mathbb{Q}(i,\alpha)\subset\mathbb{C}$. You may assume that $f=x^4-5\in K[x]$ is irreducible, and that L/K is Galois. Find $G:=\mathrm{Gal}(L/K)$, list its subgroups, and the corresponding fields between K and L. **[7]**

SOLUTION.

(a) $\mathrm{Gal}(L/K)$ is the group of field automorphisms of L which fix K pointwise.

(b) We need to prove

$$\#\operatorname{Hom}_K(L,M) \le [L:K]. \tag{1}$$

First suppose $L = K(\alpha)$ and $[L:K] = d$. Then any element of $\operatorname{Hom}_K(L,M)$ takes α to a root in M of the minimum polynomial of α, and is determined by that root. But there are at most d such roots, and (1) is proved if $L = K(\alpha)$.

We finish the proof of (1) by induction on $[L:K] = d$. It is true if $d = 1$. Let $d > 1$. Let $\alpha \in L \smallsetminus K$, $K_1 := K(\alpha)$. Then an element σ of $\operatorname{Hom}_K(L,M)$ can be given in two stages: (1) give $\sigma_1 = \sigma|_{K_1}$. There are at most $[K_1:K]$ choices for this by what we proved before. (2) Now M is a K_1-algebra and we give a K_1-homomorphism from L to M; there are at most $[L:K_1]$ choices for this by the induction hypothesis. So the total number of choices is at most $[L:K_1][K_1:K] = [L:K]$.

(c) By applying (1) to the case $M = L$ one finds $\#G \le [L:K]$. Equality when L/K is normal and separable.

(d) Proof that $H^\dagger$ is a field.

$$a, b \in L \Rightarrow \text{for all } h \in H\colon\ h(a-b) = h(a) - h(b) = a - b \Rightarrow a - b \in L.$$

Same for a/b instead of $a - b$ ($b \neq 0$) so $H^\dagger$ is a subfield of L.

Proof of $H_1 \subset H_2 \Rightarrow H_1^\dagger \supset H_2^\dagger$. Let $x \in H_2^\dagger$. In order to prove $x \in H_1^\dagger$ let $h \in H_1$. Then $h \in H_2$ so $hx = x$. This proves $x \in H_1^\dagger$. So $H_1^\dagger \supset H_2^\dagger$.

(e) We have $[L:K] = 4$ because f is irreducible. We have $\#G = [L:K] = 4$ because L/K is Galois. Any element $g \in G$ takes α to another root of f, that is, $g(\alpha) = \alpha \cdot i^t$ for some $t \in \mathbb{Z}/4$. Moreover, g is determined by t. So every $t \in \mathbb{Z}/4$ occurs precisely once for some $g \in G$. So $G \cong \mathbb{Z}/4\mathbb{Z}$; let $\sigma \in G$ be the generator with $\sigma(\alpha) = \alpha i$. Then the subgroups of G are $1, G, \langle\sigma^2\rangle$. The corresponding fields are L, K, $K(\alpha^2)$.

STATUS. (a)–(d) are bookwork. (e) is unseen but somewhat similar to examples.

5. (a) Let K be a finite field. Prove that there exists a prime number p such that K has a subfield $\mathbb{F}_p$ of p elements, and that K has p^a elements for some $a \ge 1$. **[3]**

(b) Let K be a field of characteristic $p > 0$. Prove that the map $F\colon K \to K$, $F(a) = a^p$ is a ring homomorphism. **[5]**

(c) Let $q = p^a$ be a power of a prime number p. Prove that there exists a finite field K of q elements. You may use that splitting fields exist. **[5]**

(d) Let $\mathbb{F}_p \subset L$ be a finite extension. Prove from first principles and the above results that $L/\mathbb{F}_p$ is Galois. **[7]**

(e) Find explicitly an irreducible polynomial of degree 3 over $\mathbb{F}_5$. **[5]**

SOLUTION.

(a) The prime subfield of K must be finite hence must be (isomorphic to) $\mathbb{F}_p$ for some prime number p. Now K is a vector space over $\mathbb{F}_p$ of some finite dimension a and therefore has $(\#\mathbb{F}_p)^a = p^a$ elements.

(b) Let $a, b \in K$. Clearly $F(ab) = F(a)\,F(b)$. Also

$$F(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k\, b^{p-k} = a^p + b^p = F(a) + F(b)$$

because for $0 < k < p$ we have

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!} \in p\mathbb{Z}$$

(or equals 0 if you're in K). So F is a ring homomorphism.

(c) Let K be a splitting field of $f := x^q - x$ over $\mathbb{F}_p$. Let $A \subset K$ be the set of roots in K of f. Then A is also the set of fixed points of F^a where F is the Frobenius homomorphism. Therefore, A is a subfield of K. But K is generated by A so $A = K$. Also, f has no multiple roots in any field extension because $f' = -1$. Therefore $\#K = \#A = q$.

(d) We claim that

$$\{a \in L \mid a^p - a = 0\} = \mathbb{F}_p. \tag{2}$$

It is clear that $\subset$. But $x^p - x$ has at most $p = \#\mathbb{F}_p$ roots, which proves (2).

Note that F is injective because

$$F(a) = F(b) \Rightarrow F(a-b) = 0 \Rightarrow (a-b)^p = 0 \Rightarrow a = b.$$

But L is finite so every injective map $L \to L$ is surjective. So $F \in \mathrm{Aut}(L)$. Let $G = \langle F \rangle \subset \mathrm{Gal}(L/\mathbb{F}_p)$ which is clearly finite. Then

$$L^G = \{a \in L \mid F(a) = a\} = \{a \in L \mid a^p - a = 0\} = \mathbb{F}_p$$

where the last equality is (2). So $L/\mathbb{F}_p$ is Galois.

(e) We make the following table.

$x \in \mathbb{F}_p$	0	1	2	3	4
x^3	0	1	3	2	4
$x^3 - x$	0	0	1	4	0

So $x^3 - x - 2 \in \mathbb{F}_5[x]$ has no roots and is therefore irreducible.

STATUS. (a), (b) and (c) are bookwork. (d) is unseen (unless I decide otherwise in the remaining lectures). (e) is unseen but in the same vein as many examples and sheet exercises.