Example Sheet 1, Galois Theory 2018 pmhw@dpmms.cam.ac.uk

1. Let $K \subset L$ be a field extension of degree 2. Show that if the characteristic of $K \neq 2$ then $L = K(\alpha)$ for some $\alpha \in L$ with $\alpha^2 \in K$.

*Show that if the characteristic is 2 then either $L = K(\alpha)$ for some α with $\alpha^2 \in K$, or $L = K(\alpha)$ for some α with $\alpha^2 + \alpha \in K$.

2. Let $f(t) = t^3 + t^2 - 2t + 1 \in \mathbf{Q}[t]$. Show that $f(t)$ is irreducible as a rational polynomial. Suppose that $f(t)$ is the minimal polynomial of α over the rationals. and let $\beta = \alpha^4$. Find rationals a, b, c such that $\beta = a + b\alpha + c\alpha^2$. Do the same for $\beta = (1 - \alpha^2)^{-1}$.

3. Let L/K be an extension, and $x, y \in L$ transcendental over K. Show that x is algebraic over $K(y)$ iff y is algebraic over $K(x)$. (x, y are then said to be *algebraically dependent* over K.)

4. (i) Let $K \subset L$ be a finite extension of prime degree. Show that there is no intermediate extension $K \subset M \subset L$.

(ii) Let α be such that $|K(\alpha) : K|$ is odd. Show that $K(\alpha) = K(\alpha^2)$

5. Consider the field extension $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}) = K$; show that there are precisely three intermediate fields L with $\mathbf{Q} \subset L \subset K$.

6. Find the minimal polynomial over the rationals of the following complex numbers: $(i\sqrt{3} - 1)/2$, $i + \sqrt{3}$, $\sqrt{2} + 2^{1/3}$, $\sin(2\pi/5)$, $e^{2\pi i/p}$ for p a prime.

7. Let $k(x)/k$ be a simple extension, with x transcendental over k. Show that the extension is pure transcendental, that is, the only elements of $k(x)$ which are algebraic over k are those in (the image of) k. Suppose now $K = k(a, b)$, where a is transcendental over k and $b \notin k$ but algebraic over k; prove that the extension is not simple.

8. Let L/K be a finite extension and $f(t) \in K[t]$ be an irreducible polynomial of degree $d > 1$. Show that if d and $[L : K]$ are coprime then $f(t)$ is irreducible over L.

9. Show that a regular 7-gon is not constructible by ruler and compasses.

10. If a field k is a subring of an integral domain R such that R is finite-dimensional as a k-vector space, prove that R is also a field.

11. Let K, L be subfields of a field M such that $[M : K]$ finite, and write KL for the set of all finite sums $\sum k_i l_i$ with $k_i \in K$ and $l_i \in L$. Show that KL is a subfield of M and that

$$[KL : K] \leq [L : K \cap L].$$

12. Find a splitting field F over $\mathbf{Q}$ for each of the following polynomials, and calculate $[F : \mathbf{Q}]$ in each case: $X^4 - 7X^2 + 10$, $X^4 - 7$, $X^8 - 1$, $X^3 - 2$, $X^4 + 1$. In each case, find a primitive generator for the extension (i.e. an element $x \in F$ with $F = \mathbf{Q}(x)$).

13. Let F be a finite field. By considering the multiplicative group of F, or otherwise, write down a non-constant polynomial over F which does not have a root in F. Deduce that F cannot be algebraically closed. For F the finite field with 2 elements, write down all the irreducible polynomials in $F[X]$ of degree ≤ 4.

14. *Let K_1 and K_2 be algebraically closed fields of the same characteristic. Show that either K_1 is isomorphic to a subfield of K_2 or K_2 is isomorphic to a subfield of K_1. (Use Zorn's Lemma.)

---

15. Suppose L is a degree 3 extension of a subfield K. Show that for any $\alpha \in L$ and $\beta \in L \backslash K$, we can find p, q, r, s in K such that $\alpha = \frac{p+q\beta}{r+s\beta}$.

16. Suppose k is a field and $a \in k$, and m, n are coprime integers. Show that the polynomial $X^{mn} - a$ is irreducible if and only if both $X^m - a$ and $X^n - a$ are irreducible.

17. Let L/K be a field extension, and $\phi\colon L \to L$ a K-homomorphism. Show that if L/K is algebraic then ϕ is an isomorphism. Does this hold without the hypothesis L/K algebraic?

18. Let x be algebraic over K. Show that there is only a finite number of intermediate fields $K \subset K' \subset K(x)$. [Hint: consider the minimal polynomial of x over K'.]

(ii) Show that if L/K is a finite extension of infinite fields for which there exist only finitely many intermediate subfields $K \subset K' \subset L$, then $L = K(x)$ for some $x \in L$.

19. *Show that the only field homomorphism $\mathbf{R} \to \mathbf{R}$ is the identity map.

20. *Show that for any $n > 1$ the polynomial $X^n + X + 3$ is irreducible over $\mathbf{Q}$.