Example sheet 1, Galois Theory, 2006

1. Find the greatest common divisors of the polynomials $f = X^3 - 3$ and $g = X^2 - 4$ in $\mathbb{Q}[X]$ and in $\mathbb{F}_5[X]$, expressing them in the form $af + bg$ for polynomials a, b.

2. (Quadratic extensions) Let L/K be an extension of degree 2. Show that if the characteristic of K is not 2, then $L = K(\alpha)$ for some $\alpha \in L$ with $\alpha^2 \in K$.

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

3. (i) Let L/K be a finite extension whose degree is prime. Show that there is no intermediate extension $L \supsetneqq K' \supsetneqq K$.

(ii) Let α be algebraic over K of odd degree. Show that $K(\alpha) = K(\alpha^2)$.

4. Let L/K be an extension and $\alpha, \beta \in L$. Show that if $\alpha + \beta$ and $\alpha\beta$ are algebraic over K, then α and β are also algebraic over K.

5. Let $L = K(\alpha, \beta)$, with $\deg_K \alpha = m$, $\deg_K \beta = n$, and $gcd(m, n) = 1$. Show that $[L : K] = mn$.

6. Find the minimal polynomials over $\mathbb{Q}$ of the complex numbers $\sqrt[5]{3}$, $i + \sqrt{2}$, $\sin(2\pi/5)$ and $e^{\pi i/6} - \sqrt{3}$.

7. Let α have minimal polynomial $X^3 + X^2 - 2X + 1$ over $\mathbb{Q}$. Express $(1 - \alpha^2)^{-1}$ as a linear combination of 1, α and α^2. Justify the assertion that the cubic is irreducible over $\mathbb{Q}$.

8. Let L/K be a finite extension and $f \in K[X]$ an irreducible polynomial of degree $d > 1$. Show that if d and $[L : K]$ are coprime, f has no roots in L.

9. (i) Let K be a field, and $r = p/q \in K(X)$ a non-constant rational function. Find a polynomial in $K(r)[T]$ which has X as a root.

(ii) Let L be a subfield of $K(X)$ containing K. Show that either $K(X)/L$ is finite, or $L = K$. Deduce that the only elements of $K(X)$ which are algebraic over K are constants.

10. Find a splitting field $K/\mathbb{Q}$ for each of the following polynomials, and calculate $[K : \mathbb{Q}]$ in each case:

$$X^4 - 5X^2 + 6, \quad X^4 - 7, \quad X^8 - 1, \quad X^3 - 2, \quad X^4 + 4.$$

11. Show that if L is a splitting field for a polynomial in $K[X]$ of degree n, then $[L : K] \leq n!$.

12. Write down the minimum polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Show that it is reducible mod p, for all primes p.

13. Show that an algebraic extension L/K of fields is finite if and only if it is *finitely generated*; i.e. iff $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in L$. Prove that the algebraic numbers (zeros of polynomials with rational coefficients) form a subfield of $\mathbb{C}$ which is not finitely generated over $\mathbb{Q}$.

14. Let R be a ring, and K a subring of R which is a field. Show that if R is an integral domain and $\dim_K R < \infty$ then R is a field. Show that the result fails without the assumption that R is a domain.

15. Let K and L be subfields of a field M such that M/K is finite. Denote by KL the set of all finite sums $\sum x_i y_i$ with $x_i \in K$ and $y_i \in L$. Show that KL is a subfield of M, and that

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

16. Suppose that L/K is an extension with $[L : K] = 3$. Show that for any $x \in L$ and $y \in L - K$ we can find $p, q, r, s \in K$ such that $x = \dfrac{p + qy}{r + sy}$.

[Hint: Consider four appropriate elements of the 3-dimensional vector space L.]

17. Let L/K be an extension, and $\alpha, \beta \in L$ transcendental over K. Show that α is algebraic over $K(\beta)$ iff β is algebraic over $K(\alpha)$. [α, β are then said to be **algebrically dependent**.]

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