Example sheet 2, Galois Theory, 2007

1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[K : \mathbb{Q}]$ and $Aut(K/\mathbb{Q})$.

2. Prove that every extension L/K of degree 4 with $Aut(L/K) = \mathbb{Z}/2 \times \mathbb{Z}/2$ is biquadratic.

3. Factor the following polynomials. $x^9 - x \in \mathbb{F}_3[x]$, $\quad x^{16} - x \in \mathbb{F}_4[x]$, $\quad x^{16} - x \in \mathbb{F}_8[x]$.

4. The polynomials $f(x) = x^3 + x + 1, g(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{F}_2$. Let K be the field obtained from $\mathbb{F}_2$ by adjoining a root of f, and L be the field obtained from $\mathbb{F}_2$ by adjoining a root of g. Describe explicitly an isomorphism from K to L.

5. (i) Let F be a finite field. Show that any irreducible polynomial over F is separable. More generally, show that if K is a field of characteristic $p > 0$ such that every element of K is a p^{th} power, then any irreducible polynomial over K is separable.

(ii) A field is *perfect* if every finite extension of it is separable. Show that any field of characteristic zero is perfect, and that a field of characteristic $p > 0$ is perfect if and only if every element is a p^{th} power.

6. Let K be a field of characteristic $p > 0$, and let α be algebraic over K. Show that α is separable over K if and only iff $K(\alpha) = K(\alpha^p)$.

7. Write $a_n(q)$ for the number of irreducible monic polynomials in $\mathbb{F}_q[X]$ of degree exactly n.

(i) Show that an irreducible polynomial $f \in \mathbb{F}_q[X]$ of degree d divides $X^{q^n} - X$ if and only if d divides n.

(ii) Deduce that $X^{q^n} - X$ is the product of all irreducible monic polynomials of degree dividing n, and that

$$\sum_{d|n} d a_d(q) = q^n.$$

(iii) Calculate the number of irreducible polynomials of degree 6 over $\mathbb{F}_2$.

(iv) If you know about the Möbius function $\mu(n)$, use the Möbius inversion formula to show that

$$a_n(q) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

8. 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?

9. Let K be any field and $L = K(X)$ the field of rational functions over K.

(i) Show that for any $a \in K$ there exists a unique $\sigma_a \in \mathrm{Aut}(L/K)$ such that $\sigma_a(X) = X + a$.

(ii) Let $G = \{\sigma_a \mid a \in K\}$. Show that G is a subgroup of $\mathrm{Aut}(L/K)$, isomorphic to the additive group of K. Show that if K is infinite, then $L^G = K$.

(iii) Assume that K has characteristic $p > 0$, and let $H = \{\sigma_a \mid a \in \mathbb{F}_p\}$. Show that $L^H = K(Y)$ with $Y = X^p - X$. (Use Artin's theorem.)

10. (i) Let $f \in K(X)$. Show that $K(X) = K(f)$ if and only if $f = (aX + b)/(cX + d)$ for some a, b, c, $d \in K$ with $ad - bc \neq 0$.

(ii) Show that $\mathrm{Aut}(K(X)/K) \simeq PGL_2(K)$.

11. Show that $L = \mathbb{Q}(\sqrt{2}, i)$ is a Galois extension of $\mathbb{Q}$ and determine its Galois group G. Write down the lattice of subgroups of G and the corresponding subfields of L.

12. Show that $L = \mathbb{Q}(\sqrt[4]{2}, i)$ is a Galois extension of $\mathbb{Q}$, and show that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to D_4, the dihedral group of order 8 (sometimes also denoted D_8). Write down the lattice of subgroups of D_4 (be sure you have found them all!) and the corresponding subfields of L. Which intermediate fields are Galois over $\mathbb{Q}$?

13. Let L/K be a finite Galois extension with Galois group $\{\sigma_1, \ldots, \sigma_n\}$. Show that the subset $\{\alpha_1, \ldots, \alpha_n\} \subset L$ is a K-basis for L if and only if $\det(\sigma_i(\alpha_j)) \neq 0$.

14. Let K be a field and $c \in K$. If m, n are coprime positive integers, show that $X^{mn} - c$ is irreducible if and only if both $X^m - c$ and $X^n - c$ are irreducible. (Use the Tower Law.)

15. (i) Let α be algebraic over K. Show that there is only a finite number of intermediate fields $K \subset K' \subset K(\alpha)$.

(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 $L = K(\alpha)$ for some $\alpha \in L$.