Example sheet 2, Galois Theory (Michaelmas 2005)

a.j.scholl@dpmms.cam.ac.uk

1. Find a splitting field $K/\mathbb{Q}$ for each of the following polynomials, and calculate $[K:\mathbb{Q}]$ in each case:
$$X^4 - 5X^2 + 6, \quad X^4 - 7, \quad X^8 - 1, \quad X^3 - 2, \quad X^4 + 4.$$

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

3. (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.

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

5. (i) Let K be a field of characteristic $p > 0$ and c an element of K which is not a p^{th} power. Let $n > 0$ and $q = p^n$. Show that $f(X) = X^q - c$ is irreducible in $K[X]$ and is inseparable, and that its splitting field is of the form $L = K(x)$ with $x^q = c$.

(ii) Let L/K be a finite, purely inseparable extension of fields of characteristic p. Show that if $x \in L$ then $x^{p^n} \in K$ for some $n \in \mathbb{N}$. Deduce that there is a chain of subfields $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$ where each extension K_i/K_{i-1} is of the type described in (i).

6. Let $L = \mathbb{F}_p(X,Y)$ be the field of rational functions in two variables (*i.e.* the field of fractions of $\mathbb{F}_p[X,Y]$) and K the subfield $\mathbb{F}_p(X^p, Y^p)$. Show that for any $f \in L$ one has $f^p \in K$, and deduce that L/K is not a simple extension.

7. 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?

8. Show that $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{1\}$.

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. Let L/K be a finite Galois extension with Galois group $\{\sigma_1, \ldots, \sigma_n\}$. Show that the subset $\{x_1, \ldots, x_n\} \subset L$ is a K-basis for L if and only if $\det(\sigma_i(x_j)) \neq 0$.

12. (i) Show that for any $n \geq 1$ there exists a Galois extension of fields L/K with $\mathrm{Gal}(L/K) \simeq S_n$, the symmetric group of degree n.

(ii) Show that for any finite group G there exists a Galois extension whose Galois group is isomorphic to G.

13. 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.)

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. (i) 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 $x \in L$.