Example sheet 2, Galois Theory (Michaelmas 2013)

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

This sheet covers lectures 7–12. Questions which might be more challenging are marked *.

Roots and splitting fields

1. Let $f \in K[X]$, and let $L = K(x)/K$ be an extension with $f(x) = 0$. Show that $[L : K] \leq \deg(f)$, and that equality holds if and only if f is irreducible over K.

2. Show that if f is an irreducible quadratic over the field K, and $L = K(x)$ where $f(x) = 0$, then L is a splitting field for f.

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

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

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

Separability, primitive element theorem

5. (i) Let K is a field of characteristic $p > 0$ such that every element of K is a p^{th} power. Show that any irreducible polynomial over K is separable.

(ii) Deduce that if F is a finite field, then any irreducible polynomial over F is separable.

(iii) A field is said to be *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. (i) Let K be a field of characteristic $p > 0$, and let x be algebraic over K. Show that x is inseparable over K if and only iff $K(x) \neq K(x^p)$, and that if this is the case, then p divides $[K(x) : K]$.

(ii) Deduce that if L/K is a finite inseparable extension of fields of characteristic p, then p divides $[L : K]$.

7. Let a and b be distinct rational numbers. By examining the proof of the primitive element theorem, show that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

8. 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.

Algebraic closure

9. 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.

10. * 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.)

Others

11. 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. (One way is easy. For the other, use the Tower Law.)

12. (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 $x \in L$.

13. 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?

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