Example sheet 2, Galois Theory (Michaelmas 2022)

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

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

Roots, splitting fields, normal extensions

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 $[L : K] \leq n!$.

5. Show directly from the definition that any quadratic extension is normal.

Separability, primitive element theorem

6. (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.

7. (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 $[L : K]$.

8. Let $M/L/K$ be finite extensions. Show that M is separable over K if and only if both M/L and L/K are separable extensions.

9. We say that x is *purely inseparable* over K is either $x \in K$ or $\mathrm{char}K = p > 0$ and for some $n \geq 1$, $x^{p^n} \in K$. We say that an algebraic extension L/K is purely inseparable if every element of L is purely inseparable over K.

Let L/K be a finite extension, and $L_0 = \{x \in L \mid x \text{ is separable over } K\}$. Show that L_0 is a subfield of L which is separable over K, and that L is purely inseparable over L_0.

10. Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{2\pi i/3}$. For which $a \in \mathbb{Q}$ is it the case that $K = \mathbb{Q}(\sqrt[3]{2} + a\omega)$?

11. 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 (i.e. not of the form $K(x)$).

Galois extensions

12. Which of the quadratic extensions in Q4, Sheet 1, are Galois?

13. Let L/K be a finite Galois extension, and F, F' intermediate fields.

(i) What is the subgroup of $\mathrm{Gal}(L/K)$ corresponding to the subfield $F \cap F'$?

(ii) Show that if $\sigma \colon F \xrightarrow{\sim} F'$ is a K-isomorphism, then the subgroups $\mathrm{Gal}(L/F)$, $\mathrm{Gal}(L/F')$ of $\mathrm{Gal}(L/K)$ are conjugate.

14. 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.

15. Show that $L = \mathbb{Q}(\sqrt[4]{2}, i)$ is a Galois extension of $\mathbb{Q}$, and show that $\mathrm{Gal}(L/\mathbb{Q})$ 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 $\mathbb{Q}$?

Additional examples

16. 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.)

17. (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 $x \in L$.

18. 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?

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