Groups Rings and Fields, Example Sheet 4

Dr Alessio Corti a.corti@dpmms.cam.ac.uk

March 2003

(1) (i) Let $k[\alpha]/k$ be a finite field extension of prime degree p. Take $\beta \in k[\alpha]$, $\beta \notin k$. Show that $k[\beta] = k[\alpha]$.
(ii) Suppose that $k[\alpha]/k$ is a finite field extension of degree n. Suppose that $k[\alpha^m]$ is of degree r over k. Show that $mr \geq n$.

(2) Suppose that $k[\alpha]/F$ and F/k are (finite) field extensions. Let α have minimal polynomial

$$X^m + b_{m-1}X^{m-1} + \dots b_0$$

over F. Show that

$$F = k[b_{m-1}, \dots, b_0]\,.$$

Deduce that there are only finitely many fields F with $k \leq F \leq k[\alpha]$.

(3) Find the splitting fields of the polynomials
(a) $X^3 - 2$; (b) $X^3 + 2$; (c) $X^4 - 3$; (d) $X^4 + 3$.
Determine the corresponding Galois groups, and describe how generators for the groups act on the roots.

(4) (i) What is the Galois group for $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ over $\mathbb{Q}$? What are the subgroups of the group? What are the intermediate fields? Determine which are the primitive $\alpha \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ (i.e. the α such that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$)?
(ii) Let $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}]$. Prove that $[K : \mathbb{Q}] = 8$ and find an α such that $K = \mathbb{Q}[\alpha]$. Compute the minimal polynomial of the α which you choose.

(5) (i) Let K be the splitting field of $X^4 - 4$ over $\mathbb{Q}$. Find $[K : \mathbb{Q}]$ and determine the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Find the intermediate fields, and draw a diagram showing the inclusions between them. Draw a similar diagram for the subgroups of G, and indicate which subgroup corresponds to which intermediate field.
(ii) Let K be the splitting field of $X^7 - 1$ over $\mathbb{Q}$. Find $[K : \mathbb{Q}]$ and determine the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Find the intermediate fields, and draw a diagram showing the inclusions between them. Draw a similar diagram for the subgroups of G, and indicate which subgroup corresponds to which intermediate field.

(6) [Whether or not I prove it, you may assume that the cyclotomic polynomials are irreducible over $\mathbb{Q}$.]
Take η a primitive 15th root of 1.

(i) what is the degree $[\mathbb{Q}[\eta] : \mathbb{Q}]$?
(ii) What is the degree $[\mathbb{Q}[\eta^5] : \mathbb{Q}]$?
(iii) What is the degree $[\mathbb{Q}[\eta^3] : \mathbb{Q}]$?
(iv) What is the degree $[\mathbb{Q}[\eta^2] : \mathbb{Q}]$?

What is the cyclotomic polynomial $\Phi_{15}(X)$ (that is, the minimum polynomial for η)?

(7) (i) What are the degrees of the splitting fields over $\mathbb{Q}$ of the following polynomials?
(a) $X^4 - 4X^2 + 2$. (b) $X^4 - 4X^2 + 1$. (c) $X^4 - 4X^2 - 1$.
In each case find the Galois group giving the action of generators on the roots of the polynomial.
(ii) What are the transitive subgroups of S_4? Show that the Galois group of an irreducible polynomial of the form $X^4 + aX^2 + b$ must be **either** D_8, **or** C_4 **or** $C_2 \times C_2$.

(8) Show that the Galois group of $X^5 - 2$ over $\mathbb{Q}$ contains an element of order 5 and an element of order 4, and show how such elements act on the roots. Show that the Galois group is generated by an element of order 5 and an element of order 4. Can you identify the group as a subgroup of S_5? (If you do not feel like it, then at least say how many subgroups there are of the various possible orders.)

(9) Consider the polynomial $f(X) = X^3 - 3X - 1$ over $\mathbb{Q}$.
(i) Compute the discriminant of f. [Recall that the discriminant of $X^3 + pX + q$ is $-4p^3 - 27q^2$.]
(ii) Deduce the number of real roots of f. Confirm your answer by sketching the graph.
(iii) Let K be the splitting field of f over $\mathbb{Q}$. What is $\mathrm{Gal}(K/\mathbb{Q})$?
(iv) Is K of the form $\mathbb{Q}[\alpha]$ with $\alpha^3 \in \mathbb{Q}$?
(v) Solve $f(X) = 0$. [If you keep your head you should find yourself involved with sixth roots, and then eighteenth roots of unity.]
(vi) What feature of this situation puzzled the pioneers? What can we say to them?

(10) Consider the polynomial $f(X) = X^5 - X - 1$.
(i) Show that over $\mathbb{F}_2$, f factorizes and that the Galois group is cyclic of order 6. How does a generator act on the roots?
(ii) Show that over $\mathbb{F}_3$, f is irreducible and hence the Galois group is cyclic of order 5. How does a generator act on the roots?
(iii) Deduce that the Galois group of f over $\mathbb{Q}$ is S_5.