

## Example sheet 2, Galois Theory, 2021

1. Let  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ . Determine  $[K : \mathbb{Q}]$  and  $\text{Aut}(K/\mathbb{Q})$ .
2. Prove that every extension  $L/K$  of degree 4 with  $\text{Aut}(L/K) = \mathbb{Z}/2 \times \mathbb{Z}/2$  is biquadratic.
3. Factor the following polynomials.  $x^9 - x \in \mathbb{F}_3[x]$ ,  $x^{16} - x \in \mathbb{F}_4[x]$ ,  $x^{16} - x \in \mathbb{F}_8[x]$ .
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  $p^{\text{th}}$  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  $p^{\text{th}}$  power.
6. Let  $K$  be a field of characteristic  $p > 0$ , and let  $\alpha$  be algebraic over  $K$ . Show that  $\alpha$  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
$$\sum_{d|n} da_d(q) = q^n.$$
  
(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  $\phi: L \rightarrow L$  a  $K$ -homomorphism. Show that if  $L/K$  is algebraic then  $\phi$  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  $\sigma_a \in \text{Aut}(L/K)$  such that  $\sigma_a(X) = X + a$ .  
(ii) Let  $G = \{\sigma_a \mid a \in K\}$ . Show that  $G$  is a subgroup of  $\text{Aut}(L/K)$ , 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  $\text{Aut}(K(X)/K) \simeq \text{PGL}_2(K)$ .

**11.** Let  $K$  be any field, and let  $L = K(z)$  be the function field in the variable  $z$ . Define mappings  $\sigma, \tau : L \rightarrow L$  by the formulae

$$\tau f(z) = f\left(\frac{1}{z}\right), \quad \sigma f(z) = f\left(1 - \frac{1}{z}\right).$$

Show that  $\sigma, \tau$  are automorphisms of  $L$ , and that they generate a subgroup  $G \subset \text{Aut}(L)$  isomorphic to  $S_3$ . Show that  $L^G = K(w)$  where

$$w = \frac{(z^2 - z + 1)^3}{z^2(z - 1)^2}.$$

**12.** 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  $L$ .

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

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

**15.** 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.)

**16.** (i) Let  $\alpha$  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  $\alpha \in L$ .