Separability

1. Show that every irreducible polynomial over a finite field 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 (therefore, a field of characteristic \( p > 0 \) is perfect if and only if every element is a \( p \)-th power in that field).

2. 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 if \( K(x) = K(x^p) \).

3. (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 \( P(X) = X^q - c \) is irreducible in \( K[X] \) and is inseparable, and that its splitting field is of the form \( F = K(x) \) with \( x^q = c \).
   (ii) Let \( F/K \) be a finite, purely inseparable extension (i.e. \( |\text{Hom}_K(F, E)| \leq 1 \) for every extension \( E/K \) of characteristic \( p \)). Show that if \( x \in F \) then \( x^{p^n} \in K \) for some \( n \in \mathbb{N} \). Deduce that there is a chain of subfields \( K = K_0 \subset K_1 \subset \cdots \subset K_r = F \) where each extension \( K_i/K_{i-1} \) is of the type described in (i).

4. Let \( F/K \) be a finite extension. Show that there is a unique intermediate field \( K \subset L \subset F \) such that \( L/K \) is separable and \( F/L \) is purely inseparable. (This \( K' \) is called the \textit{separable closure} of \( K \) in \( L \).)

Galois extensions

5. (i) Let \( K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \). Determine \( [K : \mathbb{Q}] \) and \( \text{Aut}_\mathbb{Q}(K) \).
   (ii) Let \( K \) be a field with \( \text{char} \ K \neq 2 \). Prove that every extension \( F/K \) with \( [F : K] = 4 \) and \( \text{Aut}_K(F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) is biquadratic, i.e. of the form \( F = K(\sqrt{a}, \sqrt{b}) \).

6. Show that \( F = \mathbb{Q}(\sqrt{2}, i) \) is a Galois extension of \( \mathbb{Q} \), and show that \( \text{Gal}(F/\mathbb{Q}) \) is isomorphic to \( D_8 \), the dihedral group of order 8 (sometimes also denoted \( D_4 \)). Write down the lattice of subgroups of \( D_8 \) (be sure you have found them all!) and the corresponding subfields of \( F \). Which subfields are Galois over \( \mathbb{Q} \)?

7. Show that all subextensions of an abelian extension are abelian.

8. (**Artin’s Theorem**) Show that a finite extension \( F/K \) is Galois if and only if \( K = F^G \) for some subgroup \( G \subset \text{Aut}_K(F) \). (In particular, the latter condition implies \( G = \text{Aut}_K(F) \) and \( [F : K] = |G| \) by the fundamental theorem.)
[Hint: for every $x \in F$, construct a separable polynomial in $F^G[X]$ of degree $\leq |G|$, whose roots lie in $F$ and are distinct, and is divisible by the minimal polynomial of $x$ over $F^G$.]

9. Let $P \in \mathbb{F}_q[X]$ be a polynomial over a finite field. Describe the Galois group of $P$ over $\mathbb{F}_q$ in terms of the irreducible factors of $P$.

10. (i) Let $F/K$ be a finite Galois extension, and $H_1$, $H_2$ subgroups of $\text{Gal}(F/K)$, with fixed fields $L_1$, $L_2$. Identify the subgroup of $\text{Gal}(F/K)$ corresponding to the field $L_1 \cap L_2$.

(ii) Show that the fixed field of $H_1 \cap H_2$ is the composite field $L_1 L_2$ of $L_1, L_2$, i.e. the subextension of $F/K$ generated by the elements of $L_1, L_2$ (or, the set of all finite sums $\sum x_i y_i$ for $x_i \in L_1$, $y_i \in L_2$; see Example Sheet 1, Problem 13).

(iii) Show $\mathbb{Q}(\mu_m) \cdot \mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{mn})$ if $m, n$ are relatively prime.

11. Let $K$ be any field and $F = K(X)$ the field of rational functions over $K$.

(i) Show that for every $a \in K$ there is a unique $\sigma_a \in \text{Aut}_K(F)$ with $\sigma_a(X) = X + a$.

(ii) Let $G = \{\sigma_a \mid a \in K\}$. Show that $G$ is a subgroup of $\text{Aut}_K(F)$, isomorphic to the additive group of $K$. Show that if $K$ is infinite, then $F^G = K$.

(iii) Assume that $K$ has characteristic $p > 0$, and let $H = \{\sigma_a \mid a \in \mathbb{F}_p\}$. Show that $F^H = K(Y)$ with $Y = X^p - X$. [Hint: use Artin’s theorem or Example Sheet 2, Problem 1.]

12. Let $K$ be any field, and let $F = K(X)$, a rational function field. Define the maps $\sigma, \tau : F \to F$ by the formulae

$$\tau f(X) = f\left(\frac{1}{X}\right), \quad \sigma f(X) = f\left(1 - \frac{1}{X}\right) \quad (\forall f \in F).$$

Show that $\sigma, \tau$ are $K$-homomorphism of $F$, and that they generate a subgroup $G \subset \text{Aut}_K(F)$ isomorphic to $S_3$. Show that $F^G = K(g)$ where

$$g(X) = \frac{(X^2 - X + 1)^3}{X^2(X - 1)^2} \in F.$$

13. Show that $\mathbb{Q}(\sqrt{2 + \sqrt{2} + \sqrt{2}})$ is an abelian extension of $\mathbb{Q}$, and determine its Galois group.

14. Use (1) the structure of $(\mathbb{Z}/(m))^\times$ (Example Sheet 2, Problem 19), (2) the **Dirichlet’s theorem on primes in arithmetic progressions**, stating that if $a$ and $b$ are coprime positive integers, then the set $\{an + b \mid n \in \mathbb{N}\}$ contains infinitely many primes, and (3) the structure theorem for finite abelian groups to show that every finite abelian group is isomorphic to a quotient of $(\mathbb{Z}/(m))^\times$ for suitable $m$. Deduce that every finite abelian group is the Galois group of some Galois extension $K/\mathbb{Q}$. [It is a long-standing unsolved problem to show this holds for an arbitrary finite group.] Find an explicit $x$ for which $\mathbb{Q}(x)/\mathbb{Q}$ is abelian with Galois group $\mathbb{Z}/23\mathbb{Z}$. 


**General equations and Kummer extensions**

15. (i) Show that for any \( n \geq 1 \) there exists a Galois extension of fields \( F/K \) with \( \text{Gal}(F/K) \cong S_n \), 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 \( G \).

16. Let \( K \) be a field containing a primitive \( n \)-th root of unity for some \( n > 1 \). Let \( a, b \in K \) such that the polynomials \( P(X) = X^n - a \) and \( Q(X) = X^n - b \) are irreducible. Show that \( P \) and \( Q \) have the same splitting field if and only if \( b = c^n a^r \) for some \( c \in K \) and \( r \in \mathbb{N} \) with \( \gcd(r, n) = 1 \).

17. (i) Let \( p \) be a prime, and \( K \) be a field with \( \text{char} K \neq p \) and \( K' := K(\mu_p) \). For \( a \in K \), show that \( X^p - a \) is irreducible over \( K \) if and only if it is irreducible over \( K' \).

(ii) If \( K \) contains a primitive \( n \)-th root of unity, then we know that \( X^n - a \) is reducible over \( K \) if and only if \( a \) is a \( d \)-th power in \( K \) for some divisor \( d > 1 \) of \( n \). Show that this need not be true if \( K \) doesn’t contain a primitive \( n \)-th root of unity.

18. Compute the Galois group of \( X^5 - 2 \) over \( \mathbb{Q} \).

**Galois groups over \( \mathbb{Q} \)**

19. (i) What are the transitive subgroups of \( S_4 \)? Find a monic polynomial over \( \mathbb{Z} \) of degree 4 whose Galois group is \( V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \).

(ii) Let \( P \in \mathbb{Z}[X] \) be monic and separable of degree \( n \). Suppose that the Galois group of \( P \) over \( \mathbb{Q} \) doesn’t contain an \( n \)-cycle. Prove that the reduction of \( P \) modulo \( p \) is reducible for every prime \( p \). (See Example Sheet 2, Problem 10.)

20. (i) Let \( p \) be prime. Show that any transitive subgroup \( G \) of \( S_p \) contains a \( p \)-cycle. Show that if \( G \) also contains a transposition then \( G = S_p \).

(ii) Prove that the Galois group of \( X^5 + 2X + 6 \) is \( S_5 \).

(iii) Show that if \( P \in \mathbb{Q}[X] \) is an irreducible polynomial of degree \( p \) which has exactly two non-real roots, then its Galois group is \( S_p \). Deduce that for an odd prime \( p \) and a sufficiently large \( m \in \mathbb{Z} \),

\[
P(X) = X^p + mp^2(X - 1)(X - 2)\cdots(X - p + 2) - p
\]

has Galois group \( S_p \).

E-mail address: t.yoshida@dpmms.cam.ac.uk