Example Sheet 3. **Lectures 13–18, Galois Theory Michaelmas 2010**

Separability

3.1. 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).

3.2. 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**, i.e. $|\mathrm{Hom}_L(F, E)| \leq 1$ for every extension E/L. (This L is called the **separable closure** of K in F.)

3.3.* 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 and only if $K(x) = K(x^p)$.

3.4.* (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 (see Problem 3.2) 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).

Galois extensions

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

3.6. (i) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[K : \mathbb{Q}]$ and $\mathrm{Aut}_{\mathbb{Q}}(K)$.

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

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

3.8. 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

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

Show that σ, τ are K-homomorphism of F, and that they generate a subgroup $G \subset \mathrm{Aut}_K(F)$ isomorphic to S_3. Using Artin's theorem, show that $F^G = K(g)$ where

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

3.9.* 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 $\sigma_a \in \mathrm{Aut}_K(F)$ with $\sigma_a(X) = X + a$.

(ii) Let $G = \{\sigma_a \mid a \in K\}$. Show that G is a subgroup of $\mathrm{Aut}_K(F)$, 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 Problem 2.5.]

3.10.* (i) Let F/K be a finite Galois extension, and H_1, H_2 subgroups of $\mathrm{Gal}(F/K)$, with fixed fields L_1, L_2. Identify the subgroup of $\mathrm{Gal}(F/K)$ 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 (see Problem 3.18 for the definition) L_1L_2 of L_1, L_2.

(iii) Show $\mathbb{Q}(\boldsymbol{\mu}_m) \cdot \mathbb{Q}(\boldsymbol{\mu}_n) = \mathbb{Q}(\boldsymbol{\mu}_{mn})$ if m, n are relatively prime.

3.11.* Determine whether the following nested radicals can be written in terms of unnested ones, and if so, find an expression: $\sqrt{2+\sqrt{11}}$, $\sqrt{6+\sqrt{11}}$, $\sqrt{11+6\sqrt{2}}$, $\sqrt{11+\sqrt{6}}$.

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

3.13.* Use (1) the structure of $(\mathbb{Z}/(m))^\times$ (Problem 2.20), (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

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

3.15. 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.

3.16. 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 $\gcd(r, n) = 1$.

3.17.* (i) Let p be a prime, and K be a field with $\operatorname{char} K \neq p$ and $K' := K(\boldsymbol{\mu}_p)$. For $a \in K$, show that $X^p - a$ is irreducible over K if and only if it is irreducible over K'. Is the result true if p is not assumed to be prime?

(ii) If K contains a primitive n-th root of unity, then show 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.

Soluble groups / Radical extensions

3.18. Let F, L be subextensions of a finite separable extension E/K. Show that if F/K and L/K are soluble, then FL/K is also soluble. Here FL is the **composite field** of F and L, i.e. the subextension of E/K generated by the elements of F, L (or, the set of all finite sums $\sum_i x_i y_i$ for $x_i \in F,\ y_i \in L$; see Problem 1.14).

3.19. Write $\cos(2\pi/17)$ explicitly in terms of radicals.

3.20.* (i) Let G be a finite group, and N its normal subgroup. Show that G is soluble if and only if N and G/N are soluble.

(ii) For a group G, the derived subgroup G^{der} is the subgroup generated by all the elements of the form $xyx^{-1}y^{-1}$ for $x, y \in G$. Show that G^{der} is normal, and that G/G^{der} is abelian (it is the **maximal abelian quotient** of G, i.e. every group homomorphism from G to an abelian group factors through G/G^{der}).

(iii) Let $G_0 = G,\ G_i = (G_{i-1})^{\mathrm{der}}$ for $i \in \mathbb{N}$. Show that G is soluble if and only if there is an i such that $G_i = \{1\}$.

(iv) Let G be the group of invertible $n \times n$ upper triangular matrices with entries in a finite field K. Show that G is soluble.

(* optional)

t.yoshida@dpmms.cam.ac.uk