Example sheet 4, Galois Theory (Michaelmas 2022)

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

Trace and norm

1. Let $L/K = \mathbb{F}_{p^r}$ be an extension of finite fields. Using the fact that L/K is Galois, generated by $\sigma = \phi_p^r$, show directly that $\mathrm{Tr}_{L/K} \colon L \to K$ is surjective. Show also that $N_{L/K}$ is surjective.

2. Let L/K be a Galois extension with cyclic Galois group of prime order p, generated by σ.

(i) Show that for any $x \in L$, $\mathrm{Tr}_{L/K}(\sigma(x) - x) = 0$. Deduce that if $y \in L$ then $\mathrm{Tr}_{L/K}(y) = 0$ if and only if there exists $x \in L$ with $\sigma(x) - x = y$.

(ii) Suppose that K has characteristic p. Use (i) to show that any element of K can be written in the form $\sigma(x) - x$ for some $x \in L$. Show also that if $\sigma(x) - x = 1$ then $a = x^p - x \in K$. Deduce that L/K is the splitting field of polynomial of the form $T^p - T - a$. (Compare this result with Q.13 on sheet 3.)

3. (Hilbert's Theorem 90). Let L/K be a Galois extension with cyclic Galois group of order $n > 1$, generated by σ.

(i) Show that if $x \in L^\times$ and $y = x/\sigma(x)$, then $N_{L/K}(y) = 1$.

(ii) Suppose that $y \in L^\times$ with $N_{L/K}(y) = 1$. Let $a_0 = 1$ and for $1 \leq k < n$, $a_k = \prod_{0 \leq i \leq k-1} \sigma^i(y)$. Show that

$$\sigma(a_k) = \begin{cases} y^{-1} a_{k+1} & \text{if } k < n-1 \\ y^{-1} a_0 & \text{if } k = n-1. \end{cases}$$

(iii) Use the theorem on the linear independence of field homomorphisms to show that there exists $z \in L$ for which

$$x = a_0 z + a_1 \sigma(z) + \cdots + a_{n-1} \sigma^{n-1}(z)$$

satisfies $y = x/\sigma(x)$.

Algebraic closure

4. Let F be a finite field. By considering the multiplicative group of F, or otherwise, write down a non-constant polynomial over F which does not have a root in F. Deduce that F cannot be algebraically closed.

5. * Let K_1 and K_2 be algebraically closed fields of the same characteristic. Show that either K_1 is isomorphic to a subfield of K_2 or K_2 is isomorphic to a subfield of K_1. (Use Zorn's Lemma.)

6. Let K be a field. By considering a suitable subfield of an algebraic closure, or otherwise, prove that there exists a separable extension K^{sep}/K in which every separable polynomial over K splits into linear factors, and that the extension K^{sep}/K is unique up to isomorphism. Show also that K^{sep}/K is a Galois extension. (K^{sep} is called a *separable closure* of K.)

7. Let K be a field. Show that a splitting field exists (and is unique up to isomorphism) for any (possibly infinite) set of polynomials over K.

Quartics

8. Let $f \in K[T]$ be a monic irreducible separable quartic, with vanishing coefficient of T^3, and let g be its resolvant cubic. Show that the discriminants of f and g are equal.

9. Let $f \in \mathbb{Q}[T]$ be an irreducible quartic polynomial whose Galois group is A_4. Show that its splitting field can be written in the form $K(\sqrt{a}, \sqrt{b})$ where $K/\mathbb{Q}$ is a Galois cubic extension and a, $b \in K$.

10. (i) Find the Galois group of $f = T^4 - 4T + 2$ over $\mathbb{Q}$,

(ii) Find the Galois group of f over $\mathbb{Q}(i)$.

Artin's Theorem

11. Show that for any finite group G there exists a Galois extension whose Galois group is isomorphic to G. (Hint: use Cayley's Theorem)

12. Let k be any field, and let $L = k(X)$. Define mappings $\sigma, \tau : L \to L$ by the formulae

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

Show that σ, τ are automorphism of L, and that they generate a subgroup $G \subset \mathrm{Aut}(L)$ isomorphic to S_3. Show that $L^H = k(g(X))$ where

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

13. 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 $\sigma_a \in \mathrm{Aut}(L/K)$ such that $\sigma_a(X) = X + a$.

(ii) Let $G = \{\sigma_a \mid a \in K\}$. Show that G is a subgroup of $\mathrm{Aut}(L/K)$, 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.)