Example Sheet 2, Galois Theory 2018 pmhw@dpmms.cam.ac.uk

1. (i) Let K be a field of characteristic $p > 0$ and let α be algebraic over K. Show that α is inseparable over K if and only if $K(\alpha)$ is not equal to $K(\alpha^p)$, and that if this is the case then p divides $|K(\alpha) : K|$. Deduce that if $K \subseteq L$ is any finite inseparable extension of fields of characteristic p then p divides $|L : K|$.

2. (i) Let $K \subseteq L$ be a finite field extension. Show that there is a unique intermediate field $K \subseteq F \subseteq L$ such that $K \subseteq F$ is separable but $F \subseteq L$ is *purely inseparable*, i.e. no element $\alpha \in L \setminus F$ is separable over F. (F is called the *separable closure* of K in L.)

(ii) Given a purely inseparable finite extension of characteristic p fields $F \subset L$ and $\alpha \in L$, show that there exists an integer $r \geq 0$ such that $\alpha^{p^r} \in F$. Deduce that if E is any extension of F, then there is at most one F-homomorphism of L into E.

3. Let $K = \mathbf{F}_p(X, Y)$ be the field of rational functions in two variables over the finite field $\mathbf{F}_p$ (that is, the field of fractions of $\mathbf{F}_p[X, Y]$), and let k denote the subfield $\mathbf{F}_p(X^p, Y^p)$. For any $g \in K$, show that $g^p \in k$, and hence deduce that the extension K/k is not simple.

4. *Suppose K, L are fields and $\sigma_1, \ldots, \sigma_m$ are distinct embedding of K into L. Prove that there do not exist elements $\lambda_1, \ldots, \lambda_m$ of L (not all zero) such that

$$\lambda_1\sigma_1(x) + \ldots + \lambda_m\sigma_m(x) = 0$$

for all $x \in K$.
[Hint : If there were a non-trivial such relation between the σ_i with $r > 1$ non-zero λ_i, show that there would also be one with s non-zero λ_i, for some $0 < s < r$.]

5. If K/k is a finite separable field extension of degree n, we consider a field extension L/k for which there are precisely n embeddings $\sigma_i : K \hookrightarrow L$ extending $k \hookrightarrow L$ (such an extension L/k exists by Theorem 3.6). Regarding k as a subfield of L, prove (cf. argument for Proposition 3.9) that for any $\alpha \in K$, we have

$$\prod_{i=1}^{n}(X - \sigma_i(\alpha)) = f^r,$$

where $r = [K : k(\alpha)]$ and f is the minimal polynomial of α over k. Deduce that

$$\mathrm{Tr}_{K/k}(\alpha) = \sum_{i=1}^{n}\sigma_i(\alpha) \quad \text{and} \quad \mathrm{N}_{K/k}(\alpha) = \prod_{i=1}^{n}\sigma_i(\alpha).$$

Using the previous question, deduce that the linear map $\mathrm{Tr}_{K/k} : K \to k$ is surjective.

6. For any finite group G, show that one can write down a Galois extension K/k, for appropriate fields K and k, such that $\mathrm{Gal}(K/k) = G$.

7. Let $K = k(X)$ be the field of rational functions over k. We define maps σ and τ by $\tau(h(X)) = h(1/X)$ and $\sigma(h(X)) = h(1 - 1/X)$ for $h \in k(X)$. Show that these are k-automorphisms of K and that they determine an action of S_3 on K. If $h(X) = \frac{(X^2-X+1)^3}{X^2(X-1)^2}$, show that h is fixed. Using Artin's Theorem, show that the fixed field is $k(h)$.

8. Show that $K = \mathbf{Q}(\sqrt{2}, i)$ is a Galois extension of $\mathbf{Q}$ and find its Galois group G. Write down the lattice of subgroups of G and the corresponding lattice of intermediate fields $\mathbf{Q} \subseteq L \subseteq K$.

9. Suppose that G is a transitive subgroup of S_p, where p is a prime, and that G contains a transposition. Prove that G contains all transpositions and hence $G = S_p$. [Hint: Define an equivalence relation $\sim$ on $\{1, 2, \ldots, p\}$ by $x \sim y$ iff $x = y$ or $(x, y) \in G$.]

If $f \in \mathbf{Q}[X]$ irreducible of degree p, with p a prime, and f has precisely two complex roots, prove that the Galois group is S_p. Considering f of the form $X^p + mp^2(X-1)(X-2)\ldots(X-(p-2)) - p$ for suitably large m, produce an example of f irreducible with Galois group S_p.

10. Show that the cubics $X^3 - 3X + c$ are irreducible over $\mathbf{Q}$ for $c = 1$ and 3; find their Galois groups. What happens when $c = 2$?

11. Show that the extension $\mathbf{Q}(2^{1/4}, i)$ over $\mathbf{Q}$ is Galois and that the Galois group has order 8. Find an element σ of order 4 in G and an element τ of order 2 which does not commute with σ. Deduce that $G \cong D_8$.

Write down the lattice of subgroups for D_8 (Warning: Most students I've supervised in the past have even got this wrong). Deduce the lattice of intermediate fields L with $\mathbf{Q} \subseteq L \subseteq \mathbf{Q}(2^{1/4}, i)$ — here each L should be explicitly described by generators, e.g. $L = \mathbf{Q}(2^{1/2}, i)$ or $L = \mathbf{Q}(2^{1/4}(i+1))$. For which of the fields L you find is $L/\mathbf{Q}$ Galois?

12. Let $\alpha = \sqrt{(2+\sqrt{2})} \in \mathbf{R}$; show that the roots of its minimal polynomial over $\mathbf{Q}$ are $\pm\alpha$ and $\pm\sqrt{(2-\sqrt{2})} = \pm\sqrt{2}/\alpha$. Deduce that $\mathbf{Q}(\alpha)$ is a Galois extension of $\mathbf{Q}$. *Find its Galois group.

---

13. If $k \subseteq K$ is a finite inseparable extension of fields, show that $\mathrm{Tr}_{K/k} : K \to k$ is the zero map (use Question 1 and the transitivity of the trace map, Lemma 3.10).

14. *Let $p_1, p_2, \ldots, p_n$ denote distinct primes, and let $L = \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$. Show that $L/\mathbf{Q}$ is Galois of degree 2^n with Galois group $(C_2)^n$. [Hint: Induction on n.]

15. Suppose that K/k is a Galois extension with Galois group $\{\sigma_1, \ldots, \sigma_n\}$. Show that $\{\beta_1, \ldots, \beta_n\}$ is a basis for K as a k-vector space if and only if $\det(\sigma_i(\beta_j)) \neq 0$.

16. Suppose that $K = k(X)$ is the field of rational functions over a field k with $\mathrm{char}(k) = p > 0$. Let $1 < n < p$ and σ the k-automorphism of K which sends X to nX. Determine the fixed field of this action.

17. If $h = f/g$ is a non-constant rational function in $k(X)$ where f, g are coprime polynomials, show that the polynomial $g(Z) - hf(Z) \in k(h)[Z]$ is irreducible. Hence deduce that $[k(X) : k(h)] = \max\{\deg(f), \deg(g)\}$. [Hint: Gauss's Lemma.]

If σ is a k-automorphism of $K = k(X)$, show that there exist $a, b, c, d \in k$ with $ad \neq bc$ such that $\sigma(X) = (aX+b)/(cX+d)$, and conversely that such elements do determine a k-automorphism of K.