Example sheet 3, Galois Theory (Michaelmas 2005)

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

1. Let M/K be a finite Galois extension, and H_1, H_2 subgroups of $\mathrm{Gal}(M/K)$, with fixed fields L_1, L_2. Find the fixed field of $H_1 \cap H_2$, and identify the subgroup of $\mathrm{Gal}(M/K)$ corresponding to the field $L_1 \cap L_2$.

2. Let M/K be a finite Galois extension, and L, L' intermediate fields. Show that if $\sigma\colon L \xrightarrow{\sim} L'$ is a K-isomorphism, then there exists $\bar\sigma \in \mathrm{Gal}(M/K)$ whose restriction to L is σ.

3. Let $L = \mathbb{F}_p(X, Y)$ be the field of rational functions in two variables (*i.e.* the field of fractions of $\mathbb{F}_p[X, Y]$) and K the subfield $\mathbb{F}_p(X^p, Y^p)$. Show that for any $f \in L$ one has $f^p \in K$, and deduce that L/K is not a simple extension.

4. (i) Let x be algebraic over K. Show that there is only a finite number of intermediate fields $K \subset K' \subset K(x)$. [Hint: Consider the minimal polynomial of x over K'.]

(ii) Let K be an infinite field, L/K a finite extension. Show that if there is only a finite number of intermediate fields $K \subset K' \subset L$ then $L = K(x)$ for some $x \in L$.

5. 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.

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

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

(ii) Let $f \in \mathbb{Z}[X]$ be monic and separable of degree n. Suppose that the Galois group of f over $\mathbb{Q}$ doesn't contain an n-cycle. Prove that the reduction of f modulo p is reducible for every prime p.

(iii) Hence exhibit an irreducible polynomial over $\mathbb{Z}$ whose reduction mod p is reducible for every p.

8. (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 $f \in \mathbb{Q}[X]$ is an irreducible polynomial of degree p which has exactly two non-real roots, then its Galois group is S_p. Deduce that for $m \in \mathbb{Z}$ sufficiently large,

$$f = X^p + mp^2(X-1)(X-2)\cdots(X-p+2) - p$$

has Galois group S_p.

9. (i) Let p be an odd prime, and let $x \in \mathbb{F}_{p^n}$. Show that $x \in \mathbb{F}_p$ iff $x^p = x$, and that $x + x^{-1} \in \mathbb{F}_p$ iff either $x^p = x$ or $x^p = x^{-1}$.

(ii) Apply (i) to a root of $X^2 + 1$ in a suitable extension of $\mathbb{F}_p$ to show that that -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$.

(iii) Show that $x^4 = -1$ iff $(x + x^{-1})^2 = 2$. Deduce that 2 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 8$.

10. Find the Galois group of $X^4 + X^3 + 1$ over each of the finite fields $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$.

11. Let p be a prime and $L = \mathbb{F}_p(X)$. Let a be an integer with $1 \le a < p$, and let $\sigma \in \mathrm{Aut}(L)$ be the unique automorphism such that $\sigma(X) = aX$. Determine the subgroup $G \subset \mathrm{Aut}(L)$ generated by σ, and its fixed field L^G.

12. Compute the Galois group of $X^5 - 2$ over $\mathbb{Q}$.

13. Let $f(X) = X^n + bX + c = \prod_{i=1}^n (X - x_i)$, with $n \ge 2$. Show that

$$x_i f'(x_i) = (n-1)b\left(\frac{-nc}{(n-1)b} - x_i\right)$$

and deduce that

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2}\left((1-n)^{n-1}b^n + n^n c^{n-1}\right).$$

14. 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

$$\sum_{d|n} d a_d(q) = q^n.$$

(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

$$a_n(q) = \frac{1}{n}\sum_{d|n} \mu(n/d) q^d.$$

15. Let K be a field of characteristic $p > 0$. Let $a \in K$, and let $f \in K[X]$ be the polynomial $f(X) = X^p - X - a$. Show that $f(X+b) = f(X)$ for every $b \in \mathbb{F}_p \subset K$. Now suppose that f does not have a root in K, and let L/K be a splitting field for f over K. Show that $L = K(x)$ for any $x \in L$ with $f(x) = 0$, and that L/K is Galois, with Galois group isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

16. (i) Let $f \in K[T]$ be a monic separable polynomial of degree n, with roots x_i in a splitting field L. Let

$$g_i(T) = \frac{f(T)}{f'(x_i)(T - x_i)} \qquad (1 \le i \le n).$$

Show that:

$$g_1 + \cdots + g_n = 1 \tag{1}$$

$$g_i g_j \equiv \begin{cases} 0 & \bmod (f) \quad \text{if } j \ne i \\ g_i & \bmod (f) \quad \text{if } j = i \end{cases} \tag{2}$$

(Equation (1) is the "partial fractions" decomposition of $1/f(T)$.)

(ii) Let L/K be a finite Galois extension with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$, with $\sigma_1 = id$. Let $x \in L$ be a primitive element with minimal polynomial $f \in K[T]$, and $x_i = \sigma_i(x)$. Let $\mathbf{A} = (A_{ij})$ be the matrix with entries $A_{ij} = \sigma_i \sigma_j g_1$. Use (2) to show that $\mathbf{A}^T\mathbf{A} \equiv \mathbf{I} \bmod (f)$.

(iii) Assume that K is infinite. Use (ii) to show that there exists $b \in K$ such that $\det(\sigma_i\sigma_j g_1(b)) \ne 0$. Deduce that if $y = g_1(b)$ then $\{\sigma(y) \mid \sigma \in G\}$ is a K-basis for L.

Such a basis $\{\sigma(y)\}$ is said to be a *normal basis* for L/K, and the result just proved is the *Normal Basis Theorem.*