Extra example sheet, Galois Theory (Michaelmas 2022)

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

These are some extra questions for those who have found the 4 example sheets too easy/short.

1. Show that the Galois group of $f = T^5 - 4T + 2$ over $\mathbb{Q}$ is S_5, and determine its Galois group over $\mathbb{Q}(i)$.

2. Suppose that $L = K(x, y)$, where x is transcendental over K and y is algebraic over K. Show that if $y \notin K$ then L/K is not a simple extension.

3. Let L/K be an infinite algebraic extension. Show that L/K is Galois if and only if $K = L^{\mathrm{Aut}(L/K)}$. [Hint: reduce to the case of a finite extension.]

4. Recall from Number Theory IIC the structure of the groups $(\mathbb{Z}/m\mathbb{Z})^\times$: if $m = \prod p^{r(p)}$ is the prime factorisation of m, then $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \prod(\mathbb{Z}/p^{r(p)}\mathbb{Z})^\times$ (by Chinese Remainder Theorem), and for prime powers we have:

— if p is odd then $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic of order $(p-1)p^{r-1}$;

— if $r \geq 2$ then $(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$.

(i) * *Dirichlet's theorem on primes in arithmetic progressions* states that if a and b are coprime positive integers, then the set $\{an + b \mid n \in \mathbb{N}\}$ contains infinitely many primes. Use this to show that every finite abelian group is isomorphic to a quotient of $(\mathbb{Z}/m\mathbb{Z})^*$ for suitable m.

(ii) 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.]

(iii) Find an explicit x for which $\mathbb{Q}(x)/\mathbb{Q}$ is abelian with Galois group $\mathbb{Z}/23\mathbb{Z}$.

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

$$g_i = \frac{f}{f'(x_i)(T - x_i)} \in L[T] \qquad (1 \leq i \leq n).$$

Show that:

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

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

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

(ii) Let L/K be a finite Galois extension with Galois group $G = \{id = \sigma_1, \ldots, \sigma_n\}$. 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 $\mathbf{A}^T\mathbf{A} \equiv \mathbf{I} \mod (f)$.

(iii) Assume that K is infinite. Use (ii) to show that there exists $b \in K$ such that $\det(\sigma_i \sigma_j g_1(b)) \neq 0$. 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*.

6. In this question, $\zeta_m = e^{2\pi i/m} \in \mathbb{C}$ for a positive integer m.

(i) Let p be an odd prime. Show that if $r \in \mathbb{Z}$ then $\sum_{0\leq s<p} \zeta_p^{rs}$ equals p if $r \equiv 0 \pmod p$ and equals 0 otherwise.

(ii) Let $\tau = \sum_{0\leq n<p} \zeta_p^{n^2}$. Show that $\tau\overline{\tau} = p$. Show also that τ is real if -1 is a square mod p, and otherwise τ is purely imaginary (i.e. $\tau/i \in \mathbb{R}$).

(iii) Let $L = \mathbb{Q}(\zeta_p)$. Show that L has a unique subfield K which is quadratic over $\mathbb{Q}$, and that $K = \mathbb{Q}(\sqrt{\varepsilon p})$ where $\varepsilon = (-1)^{(p-1)/2}$.

(iv) Show that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$ if $m|n$. Deduce that if $0 \neq m \in \mathbb{Z}$ then $\mathbb{Q}(\sqrt{m})$ is a subfield of $\mathbb{Q}(\zeta_{4|m|})$. [This is a simple case of the *Kronecker-Weber Theorem*, which states that every finite abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$.]

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

8. (i) Let $f \in K(X)$. Show that $K(X) = K(f)$ if and only if $f = (aX+b)/(cX+d)$ for some a, b, c, $d \in K$ with $ad - bc \neq 0$.

(ii) Show that $\mathrm{Aut}(K(X)/K) \simeq PGL_2(K)$.

9. * Show that for any $n > 1$ the polynomial $T^n + T + 3$ is irreducible over $\mathbb{Q}$. Determine its Galois group for $n \leq 5$.