Galois Theory: Extra Example Sheet

1. Let L/K be a finite Galois extension with Galois group $\{\sigma_1, \ldots, \sigma_n\}$. Show that the subset $\{\alpha_1, \ldots, \alpha_n\} \subset L$ is a K-basis for L if and only if $\det(\sigma_i(\alpha_j)) \neq 0$.

2. Let $\Phi_n \in \mathbb{Z}[X]$ denote the n^{th} cyclotomic polynomial. We notice that for some small values of n the coefficients of Φ_n are always -1, 0 or 1. However this is not true in general. The aim of this question is to find the smallest counterexample.

   Show that:

   (i) If n is odd then $\Phi_{2n}(X) = \Phi_n(-X)$.

   (ii) If p is a prime dividing n then $\Phi_{np}(X) = \Phi_n(X^p)$.

   (iii) If p and q are distinct primes then the nonzero coefficients of Φ_{pq} are alternately $+1$ and -1. [Hint: First show that if $1/(1-X^p)(1-X^q)$ is expanded as a power series in X, then the coefficients of X^m with $m < pq$ are either 0 or 1.]

   (iv) If n is not divisible by at least three distinct odd primes then the coefficients of Φ_n are -1, 0 or 1.

   (v) $\Phi_{3\times5\times7}$ has at least one coefficient which is not -1, 0 or 1.

3. (Hilbert's Theorem 90). Let L/K be a Galois extension with cyclic Galois group of order $n > 1$, generated by σ. The aim of this question is to show that for $y \in L^\times$ we have
$$y = x/\sigma(x) \text{ for some } x \in L^\times \iff N_{L/K}(y) = 1.$$

   (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 $1 \leqslant k < n$, let $a_k = \prod_{0 \leqslant i \leqslant k-1} \sigma^i(y)$. 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 $y = x/\sigma(x)$.

4. Let $L = k(X_1, X_2, \ldots, X_n)$ be the field of rational functions in n variables over a field k, and let $K = k(s_1, s_2, \ldots, s_n)$, where the s_i are the elementary symmetric polynomials in $X_1, \ldots, X_n$.

   (i) Let $\alpha = X_1X_2\ldots X_r$ for some $r \leqslant n$. Calculate $[K(\alpha) : K]$ and find the Galois group $\mathrm{Gal}(L/K(\alpha))$ as an explicit subgroup of S_n.

   (ii) Let $n = 4$ and $\beta = (X_1 + X_2)(X_3 + X_4)$. Calculate $[K(\beta) : K]$ and find the Galois group $\mathrm{Gal}(L/K(\beta))$ as an explicit subgroup of S_4.

5. (Inverse Galois problem for finite abelian groups) Recall from Part II Number Theory 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 the 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 $r \geqslant 2$ 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 $(\mathbb{Z}/m\mathbb{Z})^\times$ 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 α for which $\mathbb{Q}(\alpha)/\mathbb{Q}$ is abelian with Galois group $\mathbb{Z}/23\mathbb{Z}$.

6. (Normal basis theorem) The aim of this question is to show that if L/K is a finite Galois extension then L/K has a basis of the form $\{\sigma(y) \mid \sigma \in \mathrm{Gal}(L/K)\}$ for some $y \in L$. Such a basis is called a *normal basis*.

(i) Let $G = \{\mathrm{id} = \sigma_1, \ldots, \sigma_n\}$ be a finite group. Let $A = (a_{ij})$ be the $n \times n$ matrix with entries in $\mathbb{Z}[X_1, \ldots, X_n]$ such that $a_{ij} = X_k$ whenever $\sigma_i\sigma_j = \sigma_k$. Let $D(X_1, \ldots, X_n) = \det(A)$. Show that $D(1, 0, \ldots, 0) \neq 0$.

(ii) Let K be an infinite field. Show that if $F \in K[X_1, \ldots, X_n]$ is not the zero polynomial, then there exist $x_1, \ldots, x_n \in K$ with $F(x_1, \ldots, x_n) \neq 0$.

(iii) Prove that every finite Galois extension L/K has a normal basis, first in the case where K is infinite (use (i), (ii) and Question 1) and then in the case $\mathrm{Gal}(L/K)$ is cyclic (by viewing L as a $K[X]$-module and applying the structure theorem).

7. (Gauss sums) 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 $\sum_{0 \leqslant s < p} \zeta_p^{rs}$ equals p if $r \equiv 0 \pmod p$ and equals 0 otherwise.

(ii) Let $\tau = \sum_{0 \leqslant n < p} \zeta_p^{n^2}$. 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 $\mathbb{Q}(\zeta_n)$.]