Example Sheet 3, Galois Theory 2018

1. Express $\Sigma_{i \neq j} X_i^3 X_j$ as a polynomial in the elementary symmetric polynomials.

2. 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 $M = K(s_1, s_2, \ldots, s_n)$, where the $s_i$ are the elementary symmetric polynomials in $L$. Let $\alpha = X_1 X_2 \ldots X_n$ for some $r \leq n$. Calculate $[M(\alpha) : M]$ and find the Galois group $\text{Gal}(L/M(\alpha))$ as an explicit subgroup of $S_n$.

3. Let $L = K(X_1, X_2, X_3, X_4)$ be the field of rational functions in four variables over a field $K$ and let $M = K(s_1, s_2, s_3, s_4)$. Let $G$ be the dihedral subgroup of $S_4$ generated by the permutations $\sigma_1 = (1234)$ and $\sigma_2 = (13)$. Find the fixed field of $G$ in the form $M(\beta)$ for some explicit $\beta \in L$.

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

5. Give an example of a field $K$ of characteristic $p > 0$, and $\alpha$ and $\beta$ of the same degree over $K$ so that $K(\alpha)$ is not isomorphic to $K(\beta)$. Does such an example exist if $K$ is a finite field? Justify your answer.

6. Find the Galois groups of $X^5 - 15X + 21$ and $X^4 + X + 1$ over $\mathbb{Q}$.

7. Let $K = \mathbb{Q}(\zeta_n)$ be the cyclotomic field with $\zeta_n = e^{2\pi i/n}$. Show that under the isomorphism $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, complex conjugation is identified with the residue class of $-1$ (mod $n$). Deduce that if $n \geq 3$, then $[K : K \cap \mathbb{R}] = 2$ and show that $K \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos 2\pi/n)$. For which integers $n$ is it possible to construct a regular $n$-gon by ruler and compasses? (You may assume the results from Question 17.)

8. Find all four subfields of $\mathbb{Q}(e^{2\pi i/7})$. Find the quadratic subfields of $\mathbb{Q}(e^{2\pi i/15})$.

9. If $p$ is any odd prime, show that $\mathbb{Q}(e^{2\pi i/p})$ has a unique subfield of degree 2 over $\mathbb{Q}$. Let $F$ denote the cyclotomic polynomial $\Phi_p$, and $\zeta$ a primitive $p$th root of unity, show that $F'(\zeta) = p\zeta^{p-1}/(\zeta - 1)$. Prove that the norm $N_{K/\mathbb{Q}}(F'(\zeta)) = p^{p-2}$, and deduce that the unique quadratic subfield of $\mathbb{Q}(e^{2\pi i/p})$ is $\mathbb{Q}(\sqrt{k})$, where $k = (-1)^{(p-1)/2}p$.

10. Let $p$ be an odd prime. By considering the Frobenius automorphism on the splitting field of $X^2 + 1$ over $\mathbb{F}_p$, show that $-1$ is a quadratic residue mod $p$ if $p \equiv 1$ mod 4. If $\zeta$ a root of $X^4 + 1$, show that $(\zeta + \zeta^{-1})^2 = 2$. Hence show that 2 is a quadratic residue mod $p$ if $p \equiv \pm 1$ mod 8.

11. Factorize $X^9 - X$ over $\mathbb{F}_3$, and $X^{16} - X$ over both $\mathbb{F}_2$ and (harder) $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$.

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

13. How many roots does $X^5 + 27X + 16$ have over $\mathbb{Q}$, over $\mathbb{F}_3$, and over $\mathbb{F}_7$? Show that it is irreducible over $\mathbb{Q}$ and find its Galois group.

14. By showing that $2 \cos(\pi/16) = \sqrt{(2 + \sqrt{2})}$, provide another proof for the last part of Question 12 on Example Sheet 2. Show moreover that $\mathbb{Q}(\sqrt{(2 + \sqrt{(2 + \sqrt{2})})})$ is a Galois extension of $\mathbb{Q}$ and find its Galois group.
15. Let $F_q$ be the finite field of prime power order $q = p^r$. We denote by $a_n(q)$ the number of irreducible monic polynomials of degree $n$ in $F_q[X]$.

(a) Show that an irreducible polynomial $f \in F_q[X]$ of degree $m$ divides $X^{q^n} - X$ if and only if $m$ divides $n$.

(b) Show that $X^{q^n} - X$ is the product of all irreducible monic polynomials in $F_q[X]$ of degree dividing $n$.

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

(d) Use this to calculate the number of irreducible polynomials of degree 6 over $F_2$.

(e) If you know about the Möbius function $\mu(n)$, then use the Möbius inversion formula to show that
$$n a_n(q) = \sum_{d|n} \mu(n/d)q^d.$$

16. Let $\Phi_n \in \mathbb{Z}[X]$ denote the $n^{th}$ cyclotomic polynomial. 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 $\Phi_{pq}$ 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 $\Phi_n$ are $-1, 0$ or $1$.

17. In this question we determine the structure of the groups $(\mathbb{Z}/m\mathbb{Z})^\ast$.

(i) Let $p$ be an odd prime. Show that for every $n \geq 2$, $(1 + p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}$. Deduce that $1 + p$ has order $p^{n-1}$ in $(\mathbb{Z}/p^n\mathbb{Z})^\ast$.

(ii) If $b \in \mathbb{Z}$ with $(p, b) = 1$ and $b$ has order $p - 1$ in $(\mathbb{Z}/p\mathbb{Z})^\ast$ and $n \geq 1$, show that $b^{p^{n-1}}$ has order $p - 1$ in $(\mathbb{Z}/p^n\mathbb{Z})^\ast$. Deduce that for $n \geq 1$ and $p$ an odd prime, $(\mathbb{Z}/p^n\mathbb{Z})^\ast$ is cyclic.

(iii) Show that for every $n \geq 3$, $5^{2n-3} \equiv 1 + 2^{n-1} \pmod{2^n}$. Deduce that $(\mathbb{Z}/2^n\mathbb{Z})^\ast$ is generated by 5 and $-1$, and is isomorphic to $\mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, for any $n \geq 2$.

(iv) Use the Chinese Remainder Theorem to deduce the structure of $(\mathbb{Z}/m\mathbb{Z})^\ast$ in general.

(v) *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, the structure theorem for finite abelian groups, and part (iv) to show that every finite abelian group is isomorphic to a quotient of $(\mathbb{Z}/m\mathbb{Z})^\ast$ for suitable $m$. Deduce that every finite abelian group is the Galois group of some Galois extension $K/\mathbb{Q}$. Find an explicit $x$ for which $\mathbb{Q}(x)/\mathbb{Q}$ is abelian with Galois group $\mathbb{Z}/23\mathbb{Z}$. 

2