Example Sheet 3, Galois Theory 2018 pmhw@dpmms.cam.ac.uk

1. Express $\Sigma_{i\neq j}X_i^3X_j$ 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 $\alpha = X_1X_2\ldots X_r$ for some $r \leq n$. Calculate $[M(\alpha) : M]$ and find the Galois group $\mathrm{Gal}(L/M(\alpha))$ 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 $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_4$.

5. Give an example of a field K of characteristic $p > 0$, and α and β 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 $\mathbf{Q}$

7. Let $K = \mathbf{Q}(\zeta_n)$ be the cyclotomic field with $\zeta_n = e^{2\pi i/n}$. Show that under the isomorphism $\mathrm{Gal}(K/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^*$, complex conjugation is identified with the residue class of $-1 \pmod n$. Deduce that if $n \geq 3$, then $[K : K \cap \mathbf{R}] = 2$ and show that $K \cap \mathbf{R} = \mathbf{Q}(\zeta_n + \zeta_n^{-1}) = \mathbf{Q}(\cos 2\pi/n)$. 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 $\mathbf{Q}(e^{2\pi i/7})$. Find the quadratic subfields of $\mathbf{Q}(e^{2\pi i/15})$.

9. If p is any odd prime, show that $\mathbf{Q}(e^{2\pi i/p})$ has a unique subfield of degree 2 over $\mathbf{Q}$. Let F denote the cyclotomic polynomial Φ_p, and ζ a primitive pth root of unity, show that $F'(\zeta) = p\zeta^{p-1}/(\zeta - 1)$. Prove that the norm $\mathrm{N}_{K/\mathbf{Q}}(F'(\zeta)) = p^{p-2}$, and deduce that the unique quadratic subfield of $\mathbf{Q}(e^{2\pi i/p})$ is $\mathbf{Q}(\sqrt{k})$, 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 $\mathbf{F}_p$, show that -1 is a quadratic residue mod p iff $p \equiv 1 \bmod 4$. If ζ a root of $X^4 + 1$, show that $(\zeta + \zeta^{-1})^2 = 2$. Hence show that 2 is a quadratic residue mod p iff $p \equiv \pm 1 \bmod 8$.

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

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

---

13. How many roots does $X^5 + 27X + 16$ have over $\mathbf{Q}$, over $\mathbf{F}_3$, and over $\mathbf{F}_7$? Show that it is irreducible over $\mathbf{Q}$ 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 $\mathbf{Q}(\sqrt{(2 + \sqrt{(2 + \sqrt{2})})})$ is a Galois extension of $\mathbf{Q}$ and find its Galois group.

15. Let $\mathbf{F}_q$ 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 $\mathbf{F}_q[X]$.

(a) Show that an irreducible polynomial $f \in \mathbf{F}_q[X]$ 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 $\mathbf{F}_q[X]$ 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 $\mathbf{F}_2$.

(e) If you know about the Möbius function $\mu(n)$, then use the Möbius inversion formula to show that

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

16. Let $\Phi_n \in \mathbf{Z}[X]$ 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 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.

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

(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 $(\mathbf{Z}/p^n\mathbf{Z})^*$.

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

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

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

(v) **Dirichlet's theorem on primes in arithmetic progressions* states that if a and b are coprime positive integers, then the set $\{an + b \mid n \in \mathbf{N}\}$ 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 $(\mathbf{Z}/m\mathbf{Z})^*$ for suitable m. Deduce that every finite abelian group is the Galois group of some Galois extension $K/\mathbf{Q}$. Find an explicit x for which $\mathbf{Q}(x)/\mathbf{Q}$ is abelian with Galois group $\mathbf{Z}/23\mathbf{Z}$.