Galois Theory: Example Sheet 3
Michaelmas 2025

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

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

   (ii) Apply (i) to a root of $X^2 + 1$ in a suitable extension of $\mathbb{F}_p$ to show that -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$. [You have probably seen a different proof of this fact in IB GRM.]

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

3. (i) Let $u = X_1 + \omega X_2 + \omega^2 X_3$ and $v = X_1 + \omega^2 X_2 + \omega X_3$ where $\omega = e^{2\pi i/3}$. Find expressions for $u^3 + v^3$ and uv in terms of the elementary symmetric polynomials $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_1X_3 + X_2X_3$ and $s_3 = X_1X_2X_3$.
   (ii) Express $\sum_{i<j} X_i^2 X_j^2 \in \mathbb{Z}[X_1, \ldots, X_n]$ as a polynomial in the elementary symmetric polynomials.

4. Let $X_1, \ldots, X_n$ be indeterminates and set

$$A = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{pmatrix}.$$

   Show that $\det A = \prod_{1 \leqslant i < j \leqslant n} (X_j - X_i)$.
   (Hint: First show that $X_i - X_j$ is a factor of $\det A$).

5. Let L/K be an extension of finite fields. Suppose that $\#K = q$ and write σ for the q-power Frobenius. Using the fact that L/K is Galois, with Galois group generated by σ, show that the maps $\mathrm{Tr}_{L/K} \colon L \to K$ and $N_{L/K} \colon L \to K$ are surjective.

6. Let f be a monic quartic polynomial, and g its resolvent cubic. Show that the discriminants of f and g are equal.

7. (i) Let $f(X) = \prod_{i=1}^n (X - \alpha_i)$. Show that $f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$, and deduce that $\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(\alpha_i)$.
   (ii) Let $f(X) = X^n + bX + c = \prod_{i=1}^n (X - \alpha_i)$, with $n \geqslant 2$. Show that

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

   and deduce that

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

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

   (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.

9. (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.

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

11. Let $f \in \mathbb{Q}[X]$ be an irreducible quartic polynomial whose Galois group is A_4. Show that its splitting field can be written in the form $K(\sqrt{a}, \sqrt{b})$ where $K/\mathbb{Q}$ is a Galois cubic extension and a, $b \in K$. Show that the resolvent cubic of $X^4 + 6X^2 + 8X + 9$ has Galois group C_3 and deduce that the quartic has Galois group A_4.

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

    (ii) Find the Galois group of $f(X) = X^4 - 4X + 2$ over $\mathbb{Q}$ and over $\mathbb{Q}(i)$.

13. Let p be an odd prime. Show that $K = \mathbb{Q}(\zeta_p)$ has a unique subfield of degree 2 over $\mathbb{Q}$. Let $f(X) = (X^p - 1)/(X - 1)$. Show that $f'(\zeta_p) = p\zeta_p^{p-1}/(\zeta_p - 1)$ and $N_{K/\mathbb{Q}}(f'(\zeta_p)) = p^{p-2}$. Compute the discriminant of f and deduce that the unique quadratic subfield of K is $\mathbb{Q}(\sqrt{\pm p})$ for some choice of sign. How does the correct choice of sign depend on p?

Additional problems

14. 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.

15. Factor into irreducibles $X^9 - X$ over $\mathbb{F}_3$, and $X^{16} - X$ over both $\mathbb{F}_2$ and $\mathbb{F}_4$.

16. 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

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

17. Show that the Galois group of $X^5 + 20X + 16$ over $\mathbb{Q}$ is A_5.