GALOIS THEORY
Worksheet 9

Q 1. (a) Prove that the polynomials

$$f(X) = X^3 + X + 1, \quad g(X) = X^3 + X^2 + 1 \quad \in \mathbb{F}_2[X]$$

are irreducible. Consider the fields $K = \mathbb{F}_2(\alpha)$, $L = \mathbb{F}_2(\beta)$ where α, β are roots of f, g. If $\sigma\colon K \to L$ is a field isomorphism, what are the possible values of $\sigma(\alpha) \in L$ written in the basis $1, \beta, \beta^2$ of L as a $\mathbb{F}_2$-vector space? Explain why K and L are isomorphic. How many field isomorphisms $\sigma\colon K \to L$ are there?

(b) Let L be the same as in Part (a). Consider the polynomial

$$h(X) = X^4 + X + 1 \in \mathbb{F}_2[X]\ .$$

Prove that h is irreducible in $\mathbb{F}_2[X]$, or else exhibit a factorisation. Let $L \subset E$ be the splitting field of h — seen as a polynomial in $L[X]$. Is the extension $\mathbb{F}_2 \subset E$ normal? Is it separable? What is the degree $[E : \mathbb{F}_2]$? Prove that $h \in L[X]$ is irreducible, or else exhibit a factorisation.

Q 2. Show that if G is a transitive subgroup of $\mathfrak{S}_n$ containing a $(n-1)$-cycle and a transposition, then $G = \mathfrak{S}_n$.

Q 3. Consider the polynomial:

$$f(X) = X^6 - 12X^4 + 15X^3 - 6X^2 + 15X + 12$$

(a) By considering how $f(X)$ factorises in $\mathbb{F}_p[X]$ for small primes p, either prove that $f(X) \in \mathbb{Q}[X]$ is irreducible, or exhibit a factorisation.

(b) Let $\mathbb{Q} \subset K$ be the splitting field of the polynomial in (a). Determine the Galois group of the extension $\mathbb{Q} \subset K$.

Q 4. Consider the polynomial

$$f(X) = X^4 + X^2 + X + 1 \in \mathbb{Q}[X]$$

(a) By considering how $f(X)$ factorises in $\mathbb{F}_p[X]$ for small primes p, either prove that $f(X) \in \mathbb{Q}[X]$ is irreducible, or exhibit a factorisation.

(b) Let $\mathbb{Q} \subset K$ be the splitting field of the polynomial in (a). Determine the Galois group of the extension $\mathbb{Q} \subset K$.

Q 5. Consider the polynomial

$$f(X) = X^4 + 3X + 1 \in \mathbb{Q}[X]$$

(a) Show that $f(X)$ is irreducible in $\mathbb{F}_2[X]$ and compute its prime factorisation in $\mathbb{F}_5[X]$.

(b) Show that: if G is a transitive subgroup of $\mathfrak{S}_4$ that contains a 4-cycle and a 3-cycle, then $G = \mathfrak{S}_4$.

(c) Determine the structure of the Galois group of the splitting field of f over $\mathbb{Q}$.

Q 6. (a) Show that for all prime p and all integer $n > 0$ there exists an irreducible monic polynomial of degree n in $\mathbb{F}_p[X]$.

(b) Let $g(X) \in \mathbb{F}_2[X]$ be an irreducible monic polynomial of degree n; $h(X) \in \mathbb{F}_3[X]$ an irreducible monic polynomial of degree $(n-1)$; $p > n-2$ a prime and $k(X) \in \mathbb{F}_p[X]$ an irreducible monic quadratic polynomial. Show that there is a monic polynomial $f(X) \in \mathbb{Z}[X]$ with the following properties:

- $f(X) \equiv g(X) \bmod 2$,
- $f(X) \equiv Xh(X) \bmod 3$,
- $f(X) \equiv X(X+1)\cdots(X+n-3)k(X) \bmod p$.

[*Hint*: Chinese remainder theorem.]

(c) If f is the polynomial in (b), show that the Galois group of the splitting field over $\mathbb{Q}$ of f is $\mathfrak{S}_n$.