School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet V: Finite Fields

1. (a) Find an irreducible polynomial of degree 3 over $\mathbb{F}_2$ and hence construct the addition and multiplication tables of the field $\mathbb{F}_8$ of order 8.

   (b) Find an irreducible polynomial of degree 2 over $\mathbb{F}_3$ and hence construct the addition and multiplication tables of the field $\mathbb{F}_9$ of order 9.

2. Let $F \subseteq K$ be an extension of finite fields.

   (a) Show that K is a normal extension of F.

   (b) Show that K is a separable extension of F.

3. Consider the Galois field $\mathbb{F}_{p^n}$ for order p^n where p is a prime number and n is a positive integer.

   (a) If F is a subfield of $\mathbb{F}_{p^n}$, show that $F \cong \mathbb{F}_{p^d}$ for some divisor d of n. [Hint: Recall $|\mathbb{F}_{p^n} : \mathbb{F}_p| = n$.]

   (b) Suppose that d is a divisor of n.

      (i) Set $k = n/d$, $r = \sum_{i=0}^{k-1} p^{id} = (p^n - 1)/(p^d - 1)$ and
      $$g(X) = \sum_{i=1}^{r} X^{p^n - i(p^d-1)-1}.$$
      Show that
      $$g(X)\,(X^{p^d} - X) = X^{p^n} - X.$$

      (ii) Show that $\mathbb{F}_{p^n}$ contains precisely p^d roots of $X^{p^d} - X$.

      (iii) Show that $L = \{\, a \in \mathbb{F}_{p^n} \mid a^{p^d} = a \,\}$ is a subfield of $\mathbb{F}_{p^n}$ of order p^d.

   (c) Conclude that $\mathbb{F}_{p^n}$ has a unique subfield of order p^d for each divisor d of n.

4. (a) Using information about the Galois field $\mathbb{F}_{16}$ of order 16, or otherwise, factorize $X^{15} - 1$ into a product of polynomials irreducible over $\mathbb{F}_2$.

   [Hint: What are the subfields of $\mathbb{F}_{16}$? If an element lies in a particular subfield, what is the degree of its minimum polynomial?]

   (b) Using information about the Galois field $\mathbb{F}_{27}$ of order 27, or otherwise, find the degrees of the irreducible factors of $X^{26} - 1$ over $\mathbb{F}_3$. Find the number of irreducible factors of each degree.

5. A *primitive nth root of unity* in a finite field F is an element x of order n in the multiplicative group F^*. [The terminology indicates that x satisfies $x^n = 1$ and that its powers $1, x, x^2, \dots, x^{n-1}$ are the n distinct roots of $X^n - 1$ in F.]

   Let q be a power of a prime.

   (a) Show that the Galois field $\mathbb{F}_q$ of order q contains a primitive nth root of unity if and only if $q \equiv 1 \pmod{n}$.

   (b) Suppose that n and q are coprime. Show that the splitting field of $X^n - 1$ over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$ where m is minimal subject to $q^m \equiv 1 \pmod{p}$.

   (c) For each value of n in the range $1 \leqslant n \leqslant 12$, determine the degree of the splitting field of $X^n - 1$ over $\mathbb{F}_5$.

   (d) Determine for which n in the range $1 \leqslant n \leqslant 12$ does the Galois field $\mathbb{F}_{5^{36}}$ of order 5^{36} contain a primitive nth root of unity?

6. Let F be a finite field with q elements where q is odd. Prove that the splitting field of $X^4 + 1$ over F has degree one or two and that $X^4 + 1$ factorizes in $F[X]$ either as a product of four distinct linear polynomials when 8 divides $q - 1$ or as a product of two distinct quadratic irreducible polynomials when 8 does not divide $q - 1$.

   [Hint: Consider the elements $-\alpha$, $1/\alpha$ and $-1/\alpha$ where α is a root of $X^4 + 1$ in some extension of F.]

7. Let G be a finite abelian group.

   (a) If x_1 and x_2 are elements of G with coprime orders, show that $x_1 x_2$ has order given by $o(x_1 x_2) = o(x_1)\, o(x_2)$.

   (b) Suppose $p_1, p_2, \dots, p_k$ are distinct prime numbers and that $x_1, x_2, \dots, x_k \in G$ with $o(x_i) = p_i^{\alpha_i}$. Show that

$$o(x_1 x_2 \dots x_k) = o(x_1)\, o(x_2) \dots o(x_k) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

8. Give an example of a finite group (necessarily non-abelian) which has no element of order equal to its exponent.