School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet I: Rings, fields, polynomials and irreducibility

1. Write out the addition and multiplication tables for the field $\mathbb{F}_7$ of seven elements.
2. Let F be a field.
   (a) If $\{ K_i \mid i \in I \}$ is a collection of subfields of F, show that $\bigcap_{i \in I} K_i$ is a subfield of F.
   (b) Show that the prime subfield of F is the intersection of all the subfields of F.
3. Show that every finite integral domain is a field.
4. Let R be an integral domain containing a subring F that happens to be a field.
   (a) Show that R has the structure of a vector space over F.
   (b) Show that if R has finite dimension over F, then R is a field.
5. Let p be a prime number and consider the finite field $\mathbb{F}_p$ of p elements.
   (a) Show that $a^{p-1} = 1$ for all non-zero elements a in $\mathbb{F}_p$.
   (b) Show that in the polynomial ring $\mathbb{F}_p[X]$,
   $$X^p - X = X(X-1)(X-2)\dots(X-(p-1)).$$
6. Let $I = (X^4 + 1)$ be the ideal of the polynomial ring $\mathbb{F}_2[X]$ generated by the polynomial $X^4 + 1$. Let $R = F_2[X]/I$ be the quotient ring.
   (a) Show that every element of R can be expressed uniquely in the form
   $$I + (aX^3 + bX^2 + cX + d)$$
   where $a, b, c, d \in \mathbb{F}_2$.
   (b) Show that $|R| = 16$.
   (c) Show that $d \mapsto I + d$ determines an isomorphism between $\mathbb{F}_2$ and a subring of R.
   (d) Show that R can be endowed with the structure of a vector space over the field $\mathbb{F}_2$ and determine the dimenson of this vector space.
7. Show that the following polynomials are irreducible over $\mathbb{Q}$:
   (a) $X^n - p$, where n is a positive integer and p is a prime;
   (b) $X^6 + 168X^2 - 147X + 63$;
   (c) $X^3 - 3X - 1$;
   (d) $X^3 + 2X^2 - 3X + 5$.

8. Determine whether or not the following polynomials are irreducible over the given field:
   (a) $X^4 + 7$ over $\mathbb{F}_{17}$;
   (b) $X^3 - 5$ over $\mathbb{F}_{11}$.
9. Determine all the irreducible polynomials of degree at most four over the field $\mathbb{F}_2$ of two elements.
10. Find a reducible polynomial of degree 4 over the field $\mathbb{F}_2$ of two elements that has no roots in $\mathbb{F}_2$.