GALOIS THEORY: HOMEWORK 1

Due 6pm Wednesday 17th January 2024

1. Suppose that $\phi : K_1 \to K_2$ is a field isomorphism, and let $f \in K_1[t]$ be a polynomial with $\deg(f) \geq 1$. Show that f is irreducible in $K_1[t]$ if and only if $\phi(f)$ is irreducible in $K_2[t]$.
2. For each of the following pairs of polynomials f and g:
   (i) find the quotient and remainder on dividing g by f;
   (ii) use the Euclidean Algorithm to find the highest common factor h of f and g;
   (iii) find polynomials a and b with the property that $h = af + bg$.
   (a) $g = t^3 + 2t^2 - t + 3$, $f = t + 2$ over $\mathbb{F}_5$;
   (b) $g = t^7 - 4t^6 + t^3 - 4t + 6$, $f = 2t^3 - 2$ over $\mathbb{F}_7$.
3. (a) Show that $t^3 + 3t + 1$ is irreducible in $\mathbb{Q}[t]$.
   (b) Suppose that α is a root of $t^3 + 3t + 1$ in $\mathbb{C}$. Express α^{-1} and $(1 + \alpha^2)^{-1}$ as linear combinations, with rational coefficients, of 1, α and α^2.
   (c) Is it possible to express $(1+\alpha)^{-1}$ as a linear combination, with rational coefficients, of 1 and α? Justify your answer.
4. Let K be a field. Recall that the polynomial ring $K[t]$ is a unique factorisation domain. Recall also that a non-zero polynomial $f \in K[t]$ is monic if its leading coefficient is 1, meaning that $f = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ for some $a_{n-1}, \ldots, a_0 \in K$. Show that $K[t]$ contains infinitely many monic, irreducible polynomials.
   (Suggestion: First show that $K[t]$ contains at least one monic, irreducible polynomial. Then assume that $K[t]$ contains only finitely many monic, irreducible polynomials, and derive a contradiction. You might want to review Euclid's proof that there are infinitely many primes.)
5. (a) Show that the polynomial $t^2 + t + 1$ is irreducible in $\mathbb{F}_2[t]$.
   (b) Give a complete list of the coset representatives of the quotient ring $\mathbb{F}_2[t]/(t^2+t+1)$.
   (c) For each of the non-zero elements α of $\mathbb{F}_2[t]/(t^2+t+1)$, determine the least integer n (if one exists) for which $\alpha^n = 1$.