GALOIS THEORY: SOLUTIONS TO HOMEWORK 1

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 $K_2[t]$.

   Solution: Suppose that $f = gh$, where $g, h \in K_1[t]$ are polynomials with $\deg(g) \geq 1$ and $\deg(h) \geq 1$. Since ϕ is a field homomorphism (and hence is injective) we have $\phi(f) = \phi(g)\phi(h)$ with $\deg(\phi(g)) = \deg(g)$ and $\deg(\phi(h)) = \deg(h)$. Thus f is not irreducible if and only if $\phi(f)$ is not irreducible, whence f is irreducible if and only if $\phi(f)$ is irreducible.

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 $\mathbb{F}_7$.

   Solution: (a)(i) The quotient is $t^2 - 1$, and remainder 0.
   (ii) We have $g = (t^2 - 1)f$, so a highest common factor of f and g is $f = t + 2$.
   (iii) One has $f = f + 0 \cdot g$, so one may take $a = 1$ and $b = 0$.

   (b)(i) The quotient is $4t^4 - 2t^3 + 4t + 2$, and remainder $4t + 3$.
   (ii) We apply the Euclidean algorithm, noting that $g = (4t^4 - 2t^3 + 4t + 2)f + (4t + 3)$, and then $f = (4t^2 + 4t + 4)(4t + 3)$. Then a highest common factor of f and g is $4t + 3$.
   (iii) Running the Euclidean algorithm backwards, we find that

   $$4t + 3 = g - (4t^4 - 2t^3 + 4t + 2)f,$$

   so that one may take $a = 3t^4 + 2t^3 + 3t + 5$ and $b = 1$.

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.

   Solution: (a) Suppose that the polynomial $f(t) = t^3 + 3t + 1$ is reducible over $\mathbb{Q}[t]$. Then f must possess a linear factor, and hence a rational root, and the latter may be written in the form p/q with $p \in \mathbb{Z}$, $q \in \mathbb{N}$ and p and q coprime. But then $0 = q^3 f(p/q) = p^3 + 3pq^2 + q^3$, and we find that $p|q$ and $q|p$. Thus $p, q \in \{+1, -1\}$, so that $p/q = \pm 1$. The latter yields a contradiction, since $f(1) = 5$ and $f(-1) = -3$. We consequently conclude that f is irreducible over $\mathbb{Q}[t]$.

   (b) If α is a root of $t^3 + 3t + 1$ in $\mathbb{C}$, then $0 = (\alpha^3 + 3\alpha + 1)/\alpha = \alpha^2 + 3 + 1/\alpha$, whence $\alpha^{-1} = -\alpha^2 - 3$.

   We must work harder to evaluate $(1+\alpha^2)^{-1}$. We apply the Euclidean algorithm with $t^3 + 3t + 1$ and $t^2 + 1$. Thus we have

   $$\begin{aligned} t^3 + 3t + 1 &= t(t^2 + 1) + 2t + 1 \\ t^2 + 1 &= (\tfrac{1}{2}t - \tfrac{1}{4})(2t + 1) + \tfrac{5}{4}, \end{aligned}$$

whence

$$\begin{aligned}\tfrac{5}{4} &= (t^2+1) - (\tfrac{1}{2}t - \tfrac{1}{4})(2t+1)\\ &= (t^2+1) - (\tfrac{1}{2}t - \tfrac{1}{4})(t^3+3t+1-t(t^2+1))\\ &= (\tfrac{1}{2}t^2 - \tfrac{1}{4}t + 1)(t^2+1) - (\tfrac{1}{2}t - \tfrac{1}{4})(t^3+3t+1).\end{aligned}$$

Since $\alpha^3+3\alpha+1=0$, we deduce that $\frac{5}{4} = (\frac{1}{2}\alpha^2 - \frac{1}{4}\alpha + 1)(\alpha^2+1)$, whence

$$(1+\alpha^2)^{-1} = \tfrac{1}{5}(2\alpha^2 - \alpha + 4).$$

(c) No, it is not possible to express $(1+\alpha)^{-1}$ as a linear combination $a+b\alpha$ with $a,b \in \mathbb{Q}$. If $(1+\alpha)^{-1}$ were such a linear combination, then one would have $(1+\alpha)(a+b\alpha)=1$. Since α is not rational, we have $\alpha^2 = c\alpha + d$ for some $c,d \in \mathbb{Q}$. But then $-3\alpha - 1 = \alpha^3 = c\alpha^2 + d\alpha = (c^2+d)\alpha + cd$. Since α is not rational, we must have $cd = -1$ and $c^2 + d = -3$, whence $1/d^2 + d = -3$, which is to say that $d \in \mathbb{Q}$ satisfies $d^3+3d+1=0$. Since $d \in \mathbb{Q}$, we again contradict that α is not rational.

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.)

Solution: Note that t and $t+1$ are both monic, irreducible elements of $K[t]$, and so such polynomials exist. Suppose that there are only finitely many monic, irreducible elements of $K[t]$. Enumerate these polynomials as $f_1, \ldots, f_m$, and let $g = f_1 \cdots f_m + 1$. It follows that $\deg g \geq 1$, whence g is not a unit and is not 0. Thus g factors essentially uniquely as a product of irreducible elements of $K[t]$, and since g is monic, these factors may be taken to be monic. Hence, for some index j with $1 \leq j \leq m$, we have $f_j | g$. But then f_j divides $g - f_1 \ldots f_m$, meaning that f_j divides 1. This is impossible, since any multiple of f_j must have degree at least $\deg f_j \geq 1$, and $\deg 1 = 0$. We are forced to conclude that $K[t]$ must have infinitely many monic, irreducible polynomials.

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 $\alpha^n = 1$.

Solution: (a) Since $f = t^2+t+1$ has degree 2, if it is reducible then it must have a root in $\mathbb{F}_2$, but $f(0) = f(1) = 1$, so this is not the case.

(b) The elements of $\mathbb{F}_2[t]/(f)$ are the cosets $h + (f)$, where $h \in \{at+b : a,b \in \mathbb{F}_2\} = \{0, 1, t, t+1\}$.

(c) For $\alpha = 1 + (f)$, clearly $n=1$ works. For $\alpha = t + (f)$ we have $\alpha^2 = t^2 + (f) = t+1+(f)$ and $\alpha^3 = t(t+1) + (f) = 1 + (f)$, so $n = 3$ works. For $\alpha = t+1+(f)$ we have $\alpha^2 = t^2+1+(f) = t+(f)$ and $\alpha^3 = t(t+1) + (f) = 1 + (f)$, so again $n=3$ works.