**Galois theory, Problems 1**

To be handed in 11th October 2017 **SOLUTIONS**

1. 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.

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 $a = -(4t^4 - 2t^3 + 4t + 2)$ and $b = 1$.

3. (a) Show that $t^3 + 3t + 1$ is irreducible in $\mathbb{Q}[t]$.

(b) Suppose that $\alpha$ is a root of $t^3 + 3t + 1$ in $\mathbb{C}$. Express $\alpha^{-1}$ and $(1 + \alpha^2)^{-1}$ as linear combinations, with rational coefficients, of 1, $\alpha$ and $\alpha^2$.

(c) Is it possible to express $(1 + \alpha)^{-1}$ as a linear combination, with rational coefficients, of 1 and $\alpha$? 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 $\alpha$ 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 therefore deduce that

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

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 $a, b \in \mathbb{Q}$. Since $f = t^3 + 3t + 1$ is irreducible and monic, the minimal polynomial of $\alpha$ is equal to $f$. But if $(1 + \alpha)^{-1}$ were a linear combination as above, then one would have $(1 + \alpha)(a + b\alpha) = 1$, whence $b\alpha^2 + (a + b)\alpha + a - 1 = 0$. But then the minimal polynomial $f$ of $\alpha$ divides $bt^2 + (a + b)t + a - 1$, which is not possible since $\deg f > 2$.

4. Let $L : K$ be a field extension with $K \subseteq L$. Let $A \subseteq L$, and let

$$\mathcal{C} = \{C \subseteq A : C \text{ is a finite set}\}.$$

Show that $K(A) = \cup_{C \in \mathcal{C}} K(C)$, and further that when $[K(C) : K] < \infty$ for all $C \in \mathcal{C}$, then $K(A) : K$ is an algebraic extension.

Solution: The field $K(A)$ is the smallest subfield of $L$ containing $K$ and $A$. Thus, for all $C \in \mathcal{C}$, the field $K(A)$ must contain $K(C)$. So $\cup_{c \in \mathcal{C}} K(C) \subseteq K(A)$.

Now take $\gamma \in K(A)$. Then $\gamma$ is a quotient of finite $K$-linear combinations of powers of elements of $A$. Since this $K$-linear combination is finite, there is a finite set $D \subseteq A$ so that $\gamma$ is a quotient of $K$-linear combinations of powers of elements in $D$. We therefore have $D \in \mathcal{C}$ and $\gamma \in K(D)$. Thus $K(A) \subseteq \cup_{C \in \mathcal{C}} K(C)$.

We now address the final claim. Take $\alpha \in K(A)$. Then $\alpha \in K(C)$ for some $C \in \mathcal{C}$. Thus we deduce via the tower law that

$$[K(C) : K(\alpha)][K(\alpha) : K] = [K(C) : K] < \infty,$$

whence $[K(\alpha) : K] < \infty$. We therefore conclude that $\alpha$ is algebraic over $K$. Since this holds for all $\alpha \in K(A)$, we have that $K(A) : K$ is an algebraic extension.

5. Let $L : K$ be a field extension, and suppose that $\gamma \in L$ satisfies the property that $\deg m_\gamma(K) = 7$. Suppose that $h \in K[t]$ is a non-zero cubic polynomial. By noting that $\gamma$ is a root of the cubic polynomial $g(t) = h(t) - h(\gamma) \in K(h(\gamma))[t]$, show that $[K(h(\gamma)) : K] = 7$.
Solution: One has $K \subseteq K(h(\gamma)) \subseteq K(\gamma) \subseteq L$. Then by the tower law, we find that

$$[K(\gamma) : K] = [K(\gamma) : K(h(\gamma))][K(h(\gamma)) : K],$$

whence $[K(\gamma) : K(h(\gamma))]$ divides $[K(\gamma) : K]$. But the degree of the minimal polynomial of $\gamma$ over $K$ is 7, so that $[K(\gamma) : K] = 7$. We therefore see that $[K(\gamma) : K(h(\gamma))] \in \{1, 7\}$. But over the field $K(h(\gamma))$, the element $\gamma$ satisifies the cubic equation $h(t) - h(\gamma) = 0$, and thus the minimal polynomial of $\gamma$ over $K(h(\gamma))$ divides the latter cubic polynomial, so has degree 1, 2 or 3. Consequently, we must have $[K(\gamma) : K(h(\gamma))] \in \{1, 2, 3\}$. In view of our earlier observation, we are forced to conclude that the latter degree is 1, and then the previous application of the tower law implies that $[K(h(\gamma)) : K] = 7$, which is to say that the minimal polynomial of $h(\gamma)$ over $K$ has degree 7.

6. Calculate the minimal polynomial of $\sqrt[3]{7 + \sqrt[5]{21}}$ over $\mathbb{Q}$, and hence determine the degree of the field extension $\mathbb{Q}(\sqrt[3]{7 + \sqrt[5]{21}}) : \mathbb{Q}$.
Solution: Write $\alpha = \sqrt[3]{7 + \sqrt[5]{21}}$. Then $\alpha^3 - 7 = \sqrt[5]{21}$, and hence $(\alpha^3 - 7)^5 = 21$. On putting $f(x) = (x^3 - 7)^5 - 21 = x^{15} - \ldots - (7^5 + 21)$, we see that $f(\alpha) = 0$, and thus it follows that the minimal polynomial $m_\alpha(\mathbb{Q})$ of $\alpha$ divides $f$. But by applying Eisenstein's criterion using the prime 7, we see that $f$ is irreducible: the lead coefficient of $f$ is not divisible by 7, all other coefficients are divisible by 7, and the constant coefficient $-(7^5 + 21)$ is divisible by 7 but not by $7^2$. Hence $f$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$. The degree of the field extension $\mathbb{Q}(\sqrt[3]{7 + \sqrt[5]{21}}) : \mathbb{Q}$ is therefore equal to $\deg f = 15$.