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 $\alpha^n = 1$.

GALOIS THEORY: HOMEWORK 2

Due 6pm Wednesday 24th January 2024

1. Let $L : K$ be a field extension, and suppose that $\theta \in L$ satisfies the property that $[K(\theta) : K] = p$, where p is a prime number. Let
$$\alpha = c_0 + c_1\theta + \ldots + c_{p-1}\theta^{p-1},$$
for some $c_0, \ldots, c_{p-1} \in K$, and suppose that $\alpha \notin K$. By considering $[K(\alpha) : K]$, show that $K(\alpha) = K(\theta)$.

2. 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.

3. Let $L : K$ be a field extension, and suppose that $\gamma \in L$ satisfies the property that $\deg m_\gamma(K) = 5$. Suppose that $h \in K[t]$ is a non-zero cubic polynomial. By noting that γ is a root of the cubic polynomial $g(t) = h(t) - h(\gamma) \in K(h(\gamma))[t]$, show that $[K(h(\gamma)) : K] = 5$.

4. Calculate the minimal polynomial of $\sqrt[5]{7 + \sqrt[3]{21}}$ over $\mathbb{Q}$, and hence determine the degree of the field extension $\mathbb{Q}(\sqrt[5]{7 + \sqrt[3]{21}}) : \mathbb{Q}$.

5. Let $\mathbb{Q}(\alpha) : \mathbb{Q}$ be a simple field extension with the property that the minimal polynomial of α is $t^3 + 2t - 2$. Calculate the minimal polynomials of $\alpha - 1$ and $\alpha^2 + 1$ over $\mathbb{Q}$, and express the multiplicative inverses of these elements in $\mathbb{Q}(\alpha)$ in the form $c_0 + c_1\alpha + c_2\alpha^2$ for suitable rational numbers c_0, c_1, c_2.

GALOIS THEORY: HOMEWORK 3

Due 6pm Wednesday 31st January 2024

1. (a) Show that when p is a prime number, then for every positive integer n the polynomial $X^n - p$ is irreducible over $\mathbb{Q}[X]$.
   (b) By making the substitution $y = X - 1$, or otherwise, show that when p is a prime number, the polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ is irreducible over $\mathbb{Q}$.
2. (a) Show that the polynomial $\phi = t^3 - t + 1$ is irreducible over the ring $\mathbb{I} = \mathbb{F}_3[t]$.
   (b) Let $\mathbb{K} = \mathbb{F}_3(t)$. Show that the polynomial $X^{2024} + \phi X^2 + \phi$ is irreducible over $\mathbb{K}[X]$.
3. Let $L : K$ be a field extension. Suppose that $\alpha \in L$ is algebraic over K and $\beta \in L$ is transcendental over K. Suppose also that $\alpha \notin K$. Show that $K(\alpha, \beta) : K$ is not a simple field extension.
4. (a) Show that the polynomial $f(t) = t^7 - 7t^5 + 14t^3 - 7t - 2$ factorises over $\mathbb{Q}[t]$ in the form $f = g_1 g_3^2$, where $g_1, g_3 \in \mathbb{Z}[t]$ have the property that g_1 is linear, and g_3 is cubic and irreducible.
   (b) Using the identity
   $$\cos 7\theta = 64\cos^7\theta - 112\cos^5\theta + 56\cos^3\theta - 7\cos\theta,$$
   together with the conclusion of part (a), show that the angle $2\pi/7$ is not constructible by ruler and compass. Hence deduce that the regular heptagon is not constructible by ruler and compass.
5. Assume (as has in fact been proved) that $\pi = 3.14159\ldots$ is transcendental over $\mathbb{Q}$.
   (a) Show that one cannot "square the circle" – that is, prove that $\sqrt{\pi}$ is not constructible by ruler and compass.
   (b) Suppose that a generous benefactor has given you the points $(0, 0)$, $(0, 1)$ and $(0, \pi)$ in the plane. Can you now construct $\pi^{1/5}$ by ruler and compass from these three points? Explain your answer.

GALOIS THEORY: HOMEWORK 4

Due 6pm Wednesday 7th February 2024

1. (a) By considering the substitution $t = x + 1$ and applying Eisenstein's criterion, show that the polnomial $t^6 + t^3 + 1$ is irreducible over $\mathbb{Q}[t]$.
(b) Suppose, if possible, that $[\mathbb{Q}(\cos(2\pi/9), \sin(2\pi/9)) : \mathbb{Q}] = 2^r$, for some non-negative integer r. Prove that the 9-th root of unity $\omega = \cos(2\pi/9) + i\sin(2\pi/9)$ satisfies the property that $[\mathbb{Q}(\omega) : \mathbb{Q}]$ divides 2^{r+1}.
(c) By considering the factorisation of $t^9 - 1$ over $\mathbb{Q}[t]$, prove that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$. Hence deduce that the angle $2\pi/9$ is not constructible by ruler and compass, whence the regular nonagon cannot be constructed by ruler and compass.

2. (a) Suppose that $P_0, P_1, \ldots, P_n$ are points in $\mathbb{R}^2$ whose coordinates lie in a field extension K of $\mathbb{Q}$. Let $P = (x, y)$ be a point of intersection of two ellipses with equations defined over K. Explain why $[K(x, y) : K] \leq 4$.
(b) Let $P_0 = (0, 0)$ and $P_1 = (1, 0)$, and suppose that $P_2, P_3, \ldots$ are constructed successively by simple cord-and-nail constructions (as discussed in Definition 13 of section 2.3 from the notes). Let j be a positive integer, write $P_j = (x_j, y_j)$, and put $L_j = \mathbb{Q}(x_j, y_j)$. Explain why, for some non-negative integers r and s, one has $[L_j : \mathbb{Q}] = 2^r 3^s$.

3. (a) Prove that the polynomial $t^5 - 2$ is irreducible over $\mathbb{Q}[t]$.
(b) Prove that $2^{1/5}$ does not lie in any field extension L of $\mathbb{Q}$ with $[L : \mathbb{Q}] = 2^r 3^s$, for any non-negative integers r and s. (This shows that $2^{1/5}$ is not simply constructible by cord-and-nail).

4. Suppose that $L : K$ is a field extension with $K \subseteq L$, and that $\tau : L \to L$ is a K-homomorphism. Suppose also that $f \in K[t]$ has the property that $\deg f \geq 1$, and additionally that $\alpha \in L$.
(a) Show that when $f(\alpha) = 0$, then $f(\tau(\alpha)) = 0$.
(b) Deduce that when τ is a K-automorphism of L, we have that $f(\alpha) = 0$ if and only if $f(\tau(\alpha)) = 0$.

5. Let $L : K$ be a field extension. Show that $\mathrm{Gal}(L : K)$ is a subgroup of $\mathrm{Aut}(L)$.

GALOIS THEORY: HOMEWORK 5

Due 6pm Wednesday 14th February 2024

1. Suppose that $L : F$ and $L : F'$ are finite extensions with $F \subseteq L$ and $F' \subseteq L$, and further that $\psi : F \to F'$ is an isomorphism. Explain why there are at most $[L : F]$ ways to extend ψ to a homomorphism from L into L. [This is Corollary 3.6 – consider F-homomorphisms acting on L.]
2. Let M be a field. Show that the following are equivalent:
   (i) the field M is algebraically closed;
   (ii) every non-constant polynomial $f \in M[t]$ factors in $M[t]$ as a product of linear factors;
   (iii) every irreducible polynomial in $M[t]$ has degree 1;
   (iv) the only algebraic extension of M containing M is M itself.
3. Revise for the first mid-term!

GALOIS THEORY: HOMEWORK 6

Due 6pm Wednesday 21st February 2024

1. Suppose that L and M are fields with an associated homomorphism $\psi : L \to M$. Show that whenever L is algebraically closed, then $\psi(L)$ is also algebraically closed.
2. Let $L : K$ be a field extension with $K \subseteq L$. Let $\gamma \in L$ be transcendental over K, and consider the simple field extension $K(\gamma) : K$. Show that $K(\gamma)$ is not algebraically closed.

GALOIS THEORY: HOMEWORK 7

Due 6pm Wednesday 28th February 2024

1. Suppose that $\overline{K}$ is an algebraic closure of K, and assume that $K \subseteq \overline{K}$. Take $\alpha \in \overline{K}$ and suppose that $\sigma : K \to \overline{K}$ is a homomorphism.
   (a) Show that σ can be extended to a homomorphism $\tau : \overline{K} \to \overline{K}$.
   (b) Prove that the number of distinct roots of $m_\alpha(K)$ in $\overline{K}$ is equal to the number of distinct roots of $\sigma(m_\alpha(K))$ in $\overline{K}$.
2. Suppose that $L : K$ is an algebraic extension of fields.
   (a) Show that $\overline{L}$ is an algebraic closure of K, and hence $\overline{L} \simeq \overline{K}$.
   (b) Suppose that $K \subseteq L \subseteq \overline{L}$. Show that one may take $\overline{K} = \overline{L}$.
3. For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.
   (a) $t^3 - 1$
   (b) $t^7 - 1$
4. For each of the following polynomials, construct a splitting field L over $\mathbb{Q}$ and compute the degree $[L : \mathbb{Q}]$.
   (a) $t^4 + t^2 - 6$
   (b) $t^8 - 16$
5. Suppose that $L : K$ is a splitting field extension for the polynomial $f \in K[t] \setminus K$.
   (a) Prove that $[L : K] \leq (\deg f)!$.
   (b) Prove that $[L : K]$ divides $(\deg f)!$.

GALOIS THEORY: HOMEWORK 8

Due 6pm Wednesday 6th March 2024

1. Recall the splitting field L over $\mathbb{Q}$ that you constructed in question 4(b) of Problem Sheet 7 for the polynomial $t^8 - 16$. Determine the subgroup of S_4 to which $\mathrm{Gal}(L : \mathbb{Q})$ is isomorphic.
2. Suppose that K is a field and that $L : K$ is a splitting field extension for an irreducible polynomial $f \in K[t]$ of degree n. Assume that $K \subseteq L$.
   (a) Show that whenever α and β are roots of f in L, and σ is a K-automorphism of L, then $\sigma(\alpha) = \sigma(\beta)$ if and only if $\alpha = \beta$;
   (b) Show that the elements of $\mathrm{Gal}(L : K)$ act as permutations on the n roots of f, and hence deduce that $\mathrm{Gal}(L : K)$ has order dividing $n!$;
   (c) Let g be a degree m polynomial in $K[t]$, not necessarily irreducible, and let $M : K$ be a splitting field extension for g. Show that $|\mathrm{Gal}(M : K)|$ divides $m!$.
3. Suppose that $L : K$ is a normal extension, and that $K \subseteq L \subseteq \overline{K}$. Recall that since $L : K$ is algebraic, then any algebraic closure of K is an algebraic closure of L.
   (a) Show that for any K-homomorphism $\tau : L \to \overline{K}$, one has $\tau(L) = L$;
   (b) Suppose that M is a field satisfying $K \subseteq M \subseteq L$. Show that $L : M$ is a normal extension.
4. Which of the following field extensions are normal? Justify your answers.
   (a) $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$
   (b) $\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}$
   (c) $\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}$
   (d) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$
   (e) $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$.
5. Let $K = \mathbb{F}_5(t)$. Find an algebraic field extension $L : K$ which is not normal, and justify your answer.

GALOIS THEORY: HOMEWORK 9

Due 6pm Wednesday 20th March 2024

1. Suppose that $E : K$ and $F : K$ are finite extensions having the property that K, E and F are contained in a field L.
   (a) Show that $EF : K$ is a finite extension;
   (b) Show that when $E : K$ and $F : K$ are both normal, then $E \cap F : K$ is a normal extension;
   (c) Show that when $E : K$ and $F : K$ are both normal, then $EF : E \cap F$ is a normal extension.
2. Suppose that $L : M$ is an algebraic extension with $M \subseteq L$. Show that when $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism, then $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$ if and only if $m_\alpha(M)$ is separable over M.
3. (a) Suppose that $f \in K[t]$ is separable over K and that $L : K$ is a splitting field extension for f. Show that $L : K$ is separable.
   (b) Suppose that $L : K$ is a splitting field extension for $S \subseteq K[t]$ where each $f \in S$ is separable over K. Show that $L : K$ is a separable extension.
4. Let p be a prime number, let $\mathbb{F}_p$ denote the finite field of p elements, and let $K = \mathbb{F}_p(t)$. Suppose that $L : K$ is a field extension, and $s \in L$ is transcendental over K.
   (a) Write $J = K(s)$, and let E denote a splitting field for the polynomial $x^p - t \in J[x]$. Show that for some $\xi \in E$, one has $x^p - t = (x - \xi)^p$, and deduce that $[E : J] = p$.
   (b) Let $U : J$ be a splitting field extension for the polynomial $(x^p - t)(x^p - s)$. By considering a splitting field extension F for the polynomial $x^p - s \in E[x]$, show that $[U : J] = p^2$.
5. With the same notation as in the previous question:
   (a) Show that if $\gamma \in U$, then $\gamma^p \in J$.
   (b) What is the degree of the field extension $J(\gamma) : J$? Explain.
   (c) Deduce that $U : J$ is a finite field extension which is not simple.

GALOIS THEORY: HOMEWORK 10

Due 6pm Wednesday 27th March 2024

1. Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f. Assume that $K \subseteq L$.
   (a) Show that when f has a repeated root over L, then there exists $\alpha \in L$ for which $f(\alpha) = 0 = (Df)(\alpha)$.
   (b) Show that when $\alpha \in L$ satisfies $f(\alpha) = 0 = (Df)(\alpha)$, then there exists $g \in K[t]$ having the property that $\deg g \geq 1$ and g divides both f and Df.
   (c) Show that when $g \in K[t] \setminus K$ divides both f and Df, then f has a repeated root over L.
2. Suppose that $\mathrm{char}(K) = p > 0$ and f is irreducible over $K[t]$.
   (a) Show that there is an irreducible and separable polynomial $g \in K[t]$ and a non-negative integer n with the property that $f(t) = g(t^{p^n})$.
   (b) Let $L : K$ be a splitting field extension for f. Show that there exists a non-negative integer n with the property that every root of f in L has multiplicity p^n.
3. Revise for the second mid-term!

GALOIS THEORY: HOMEWORK 11

Due 6pm Wednesday 3rd April 2024

1. Suppose that $L : M : K$ is an algebraic tower of fields. Prove that $L : K$ is separable if and only if $L : M$ and $M : K$ are both separable. [Hint: try using the Primitive Element Theorem].
2. Suppose that $E : K$ and $F : K$ are finite extensions with $K \subseteq E \subseteq L$ and $K \subseteq F \subseteq L$, with L a field.
   (a) Show that when $E : K$ is separable, then so too is $EF : F$.
   (b) Show that when $E : K$ and $F : K$ are both separable, then so too are $EF : K$ and $E \cap F : K$.
3. Suppose that $\mathrm{char}(K) = p > 0$ and that $L : K$ is a totally inseparable algebraic extension (thus, every element of $L \setminus K$ is inseparable). Show that whenever $\alpha \in L$, then there is a non-negative integer n and an element $\theta \in K$ having the property that $m_\alpha(K) = t^{p^n} - \theta$.

GALOIS THEORY: HOMEWORK 12

Due 6pm Wednesday 10th April 2024

1. Let $L : K$ be a finite Galois extension with Galois group G. For any $\alpha \in L$, define the polynomial $f_\alpha(t) = \prod_{\sigma \in G}(t - \sigma(\alpha))$.
   (a) Show that $f_\alpha \in K[t]$.
   (b) Prove that if $\sigma(\alpha) \neq \tau(\alpha)$ whenever $\sigma, \tau \in G$ satisfy $\sigma \neq \tau$, then $f_\alpha = m_\alpha(K)$.
2. Use question 1 to calculate the minimal polynomial of $2\sqrt{-3} - \sqrt{2}$ over $\mathbb{Q}$.
3. Let f denote the polynomial $t^3 + t + 1$.
   (a) Write down a splitting field extension for f over $\mathbb{F}_2$.
   (b) What is $\mathrm{Gal}_{\mathbb{F}_2}(f)$? Justify your answer, and determine all subfields of the splitting field that you wrote down in part (a).
4. Let f denote the polynomial $t^4 + t^3 + t^2 + t + 1$.
   (a) Write down a splitting field extension for f over $\mathbb{Q}$.
   (b) Show that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong C_4$, where C_4 is the cyclic group of order 4.
5. Use the Galois correspondence to determine all subfields of the splitting field that you wrote down in part (a) of question 4. Draw the lattice of subfields and corresponding lattice of subgroups of C_4.

GALOIS THEORY: HOMEWORK 13

Due 6pm Wednesday 17th April 2024

1. Let f denote the polynomial $t^3 - 7$.
   (a) Write down a splitting field extension for f over $\mathbb{Q}$.
   (b) Show that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_3$.
2. Use the Galois correspondence to determine all subfields of the splitting field that you wrote down in part (a) of question 1. Draw the lattice of subfields and corresponding lattice of subgroups of S_3.
3. Suppose that L is a finite field having p^n elements, where p is a prime number. Recall that $\mathrm{Gal}(L : \mathbb{F}_p) = \langle \varphi \rangle$, where φ denotes the Frobenius mapping.
   (a) Show that whenever K is a subfield of L, then $|K| = p^d$ for some divisor d of n.
   (b) Show that for each divisor d of n, there is a unique subfield K of L with $|K| = p^d$.
4. Let $L : K$ be a finite Galois extension with Galois group G.
   (a) For any $\alpha \in L$, define the *norm* of α by $\mathrm{N}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. Show that $\mathrm{N}(\alpha) \in K$.
   (b) For any $\alpha \in L$, define the *trace* of α by $\mathrm{Tr}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha)$. Show that $\mathrm{Tr}(\alpha) \in K$.
5. Let p be a prime number, and n a natural number, and denote by $\mathbb{F}_q$ the finite field of $q = p^n$ elements with prime field $\mathbb{F}_p$. Let ϕ denote the Frobenius monomorphism from $\mathbb{F}_q$ into $\mathbb{F}_q$. Recall that $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = \langle \phi \rangle$.
   (a) Defining the trace of $\alpha \in \mathbb{F}_q$ as in question 4(b) above, show that there exists an element $\alpha \in \mathbb{F}_q$ having non-zero trace.
   (b) Defining the norm of $\alpha \in \mathbb{F}_q$ as in question 4(a) above, show that there exists a non-zero element $\alpha \in \mathbb{F}_q^{\times}$ having norm different from 1.

GALOIS THEORY: HOMEWORK 14

Not for assessment – solutions will be provided

1. (a) Show that $f = t^3 - 3t + 1$ is irreducible over $\mathbb{Q}$.
   (b) Show that whenever α is a root of f in a splitting field extension of $\mathbb{Q}$, then $\beta = \alpha^2 - 2$ is also a root of f.
   (c) Let L be a splitting field for f over $\mathbb{Q}$. Use your answer to part (b) to show that $[L : \mathbb{Q}] = 3$, and conclude that the Galois group of f is isomorphic to $A_3 \cong C_3$.
   (d) Show that there is no $\gamma \in L$ such that $\gamma \notin \mathbb{Q}$ and $\gamma^3 \in \mathbb{Q}$, and conclude that $L : \mathbb{Q}$ is not a radical extension.
   (e) By Cardano's formula, the equation $f = 0$ is soluble by radicals. How do you reconcile this observation with your answer to part (d)?
2. Is the polynomial $t^5 - 4t^4 + 2$ soluble by radicals over $\mathbb{Q}$?
3. Is the polynomial $t^6 - 4t^2 + 2$ soluble by radicals over $\mathbb{Q}$?
4. Let n be a positive integer and K a field with characteristic not dividing n. Let $L = K(\zeta)$, where ζ is a primitive nth root of unity.
   (a) Show that $\mathrm{Gal}(L : K)$ is isomorphic to a subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$.
   (b) Show that if n is prime and $K = \mathbb{Q}$ then either $L = K$ or $\mathrm{Gal}(L : K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
5. Let n be a positive integer. By Dirichlet's theorem, there exists a prime number p with $p \equiv 1 \pmod{n}$.
   (a) Let $L = \mathbb{Q}(e^{2\pi i/p})$. Show that $\mathrm{Gal}(L : \mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.
   (b) Show that $\mathbb{Q}(e^{2\pi i/p})$ contains a subfield M with the property that $\mathrm{Gal}(M : \mathbb{Q}) \cong C_n$.