1. Let $K \subseteq L$ be fields, and $\alpha \in L$. We understand the structure of $K(\alpha)$ when α is algebraic over K. In this question we will deal with the case that α is transcendental over K.

Suppose that α is transcendental over K and let $\varphi_\alpha \colon K[x] \longrightarrow L$ be the evaluation map sending $f(x) \in K[x]$ to $f(\alpha) \in L$. Recall that this is a ring homomorphism.

(a) Explain why φ_α is injective.

(b) Explain how to use φ_α to get a homomorphism of fields $K(x) \longrightarrow L$. (Suggestion: It is just like our argument that $\mathbb{Q}$ is a subfield of every field of characteristic 0, starting from the point where we know that $\mathbb{Z}$ is a subring of every such field.)

(c) Prove that $K(\alpha) \cong K(x)$.

(d) Are $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ isomorphic fields? (Here $\pi \cong 3.14159265\ldots$ and $e \cong 2.718281828\ldots$ are the usual numbers we know.)

Solution.

(a) Since α is transcendental over K, the only polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$ is the zero polynomial. Thus φ_α is injective.

(b) Define a map $\psi_\alpha \colon K(x) \longrightarrow L$ by

$$\psi_\alpha\left(\frac{f(x)}{g(x)}\right) = \frac{\varphi_\alpha(f(x))}{\varphi_\alpha(g(x))} = \frac{f(\alpha)}{g(\alpha)}.$$

Since $g(\alpha) \neq 0$ whenever $g(x) \neq 0$, this map is well defined. Furthermore, since φ_α is a ring homomorphism it follows immediately from the rules for addition and multiplication in the ring of fractions that ψ_α is a ring homomorphism too. This map is not the zero map since $\psi_\alpha(1) = 1 \neq 0$. Therefore this map is an injective map of fields, and $\mathrm{Im}(\psi_\alpha) \cong K(x)$.

(c) The image of ψ_α consists of all expressions of the form

$$(\dagger) \qquad \frac{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_d\alpha^d}{b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_e\alpha^e}$$

where $b_0 + b_1x + \cdots + b_ex^e$ is not the zero polynomial, i.e., not all of the b_j are zero.

From the description, $\mathrm{Im}(\psi_\alpha)$ is a field which contains K and α, and therefore (by the definition of $K(\alpha)$) contains $K(\alpha)$.

On the other hand, we have $K \subset K(\alpha)$ and $\alpha \in K(\alpha)$, and so all expressions which can be built from α and elements of K using the field operations are in $K(\alpha)$. In particular, all expressions of the form (†) are in $K(\alpha)$ and therefore $\mathrm{Im}(\psi_\alpha) \subseteq K(\alpha)$. Thus $K(x) \cong \mathrm{Im}(\psi_\alpha) = K(\alpha)$.

(d) Since both π and e are transcendental over $\mathbb{Q}$, By part (c) we have $\mathbb{Q}(\pi) \cong K(x) \cong \mathbb{Q}(e)$, and so $\mathbb{Q}(\pi)$ and $\mathbb{Q}(e)$ are isomorphic fields.

2. Let p be a prime, n a positive integer, and write $n = mp^k$ with $p \nmid m$. For any a, $0 \leqslant a \leqslant n$, prove that

$$\binom{n}{a} \equiv \begin{cases} 0 & \mod p \quad \text{if } p^k \nmid a \\ \left(\begin{array}{c} m \\ \frac{a}{p^k} \end{array}\right) & \mod p \quad \text{if } p^k \mid a. \end{cases}$$

(Suggestion: Consider $(x+1)^n \bmod p$, i.e, in $\mathbb{F}_p$.)

Solution. By the binomial theorem we have

$$(x+1)^n = \sum_{a=0}^{n} \binom{n}{a} x^a,$$

while mod p (i.e., in $\mathbb{F}_p$) we have

$$(x+1)^n = (x+1)^{p^k m} = \left((x+1)^{p^k}\right)^m = (x^{p^k}+1)^m = \sum_{b=0}^{m} \binom{m}{b} \left(x^{p^k}\right)^b = \sum_{b=0}^{m} \binom{m}{b} x^{b \cdot p^k}.$$

Since the second equation only has powers of p^k, comparing coefficients gives $\binom{n}{a} \equiv 0 \pmod{p}$ if $p^k \nmid a$. On the other hand, if a is divisible by p^k, if we write $a = b \cdot p^k$ (or equivalently, that $b = \frac{a}{p^k}$) then comparing coefficients gives $\binom{n}{a} \equiv \binom{m}{b} \pmod{p}$. These two formulas were exactly what we wanted to prove. □

3. Let K be a field with $\mathrm{Char}(K) \neq 2$ and suppose that L/K is a degree 2 extension. By the argument in class, that means we can express L as $K(\sqrt{\gamma})$ for some $\gamma \in K$. In class we showed that L/K must be a normal extension.

(a) Show that L/K is also a separable extension.

(b) Compute $\mathrm{Aut}(L/K)$ and describe how each element of the group acts on L.

Solution. From class we have seen that

$$L = K(\sqrt{\gamma}) = \left\{ a + b\sqrt{\gamma} \,\middle|\, a, b, \in K \right\}.$$

(a) Given $\alpha = a + b\sqrt{\gamma} \in L$ (with both $a, b \in K$), then we consider two cases. If $b = 0$ then $\alpha \in K$ with minimal polynomial $x - \alpha \in K[x]$. Since this polynomial only has one root, α is separable over K. If $b \neq 0$ then let

$$q(x) = (x - (a + b\sqrt{\gamma})) \cdot (x - (a - b\sqrt{\gamma})) = x^2 - 2ax + (a^2 - b^2\gamma) \in K[x].$$

This polynomial has roots $\alpha = a + b\sqrt{\gamma}$ and $a - b\sqrt{\gamma}$. Since $b \neq 0$ these roots are distinct, and again α is separable over K. Since all elements of L are separable over K, L/K is a seperable extension.

(b) By our bound on the autmorphism group, we have $|\operatorname{Aut}(L/K)| \leqslant [L : K] = 2$, so that either $|\operatorname{Aut}(L/K)| = 1$ and $\operatorname{Aut}(L/K)$ is the trivial group, or $|\operatorname{Aut}(L/K)| = 2$ and $\operatorname{Aut}(L/K)$ is the group of order 2. We always have $\mathrm{Id}_L \in \operatorname{Aut}(L/K)$, and we will show that $\operatorname{Aut}(L/K) = 2$ by finding a second autmorphism of L/K.

The polynomial $q(x) = x^2 - \gamma \in K[x]$ has $\sqrt{\gamma}$ as a root. Any automorphism σ of L/K therefore has to take $\sqrt{\gamma}$ to a root of $q(x)$, so $\sigma(\sqrt{\gamma})$ must be either $\pm\sqrt{\gamma}$. We will now check that the map $\sigma : L \longrightarrow L$ given by $\sigma(a + b\sqrt{\gamma}) = a - b\sqrt{\gamma}$ is an autmorphism of L fixing K.

From the formula, σ is given by a K-linear map, whose matrix in the K-basis 1, $\sqrt{\gamma}$ of L is

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

This matrix has determinant -1 and so is invertible. Thus σ is a bijection from L to L compatible with addition. (From the formula for σ or the matrix we also see that $\sigma^2 = \mathrm{Id}_L$, i.e, σ has order 2.) We now check that σ is compatible with multiplication.

Given $\alpha = a + b\sqrt{\gamma}$ and $\beta = c + d\sqrt{\gamma} \in L$ (with $a, b, c, d \in K$), we have $\alpha\beta = (ac + bd\gamma) + (ad + bc)\sqrt{\gamma}$, and so

$$\begin{aligned} \sigma(\alpha) \cdot \sigma(\beta) &= (a - b\sqrt{\gamma}) \cdot (c - d\sqrt{\gamma}) = (ac + (-b)(-d)\gamma) + (a(-d) + (-b)c)\sqrt{\gamma} \\ &= (ac + bd\gamma) - (ad + bc)\sqrt{\gamma}, \end{aligned}$$

while

$$\sigma(\alpha \cdot \beta) = \sigma\left((ac + bd\gamma) + (ad + bc)\sqrt{\gamma}\right) = (ac + bd\gamma) - (ad + bc)\sqrt{\gamma}.$$

Comparing these two formulas we get $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta)$. Therefore σ is also compatible with multiplication. From the formula for σ we also see that σ fixes K. Therefore $\sigma \in \operatorname{Aut}(L/K)$. If $b \neq 0$ then $\sigma(a + b\sqrt{\gamma}) = a - b\sqrt{\gamma} \neq a + b\sqrt{\gamma}$, and so $\sigma \neq \mathrm{Id}_L$. Therefore $\operatorname{Aut}(L/K)$ is the group of order 2.

REMARK. We have seen already that L/K is a normal extension. Therefore by part (a) L/K is a separable normal extension, i.e., a Galois extension. By our theorem characterizing Galois extensions this implies that $|\operatorname{Aut}(L/K)| = [L : K]$, something we have explicitly verified in this case.

4. In class we saw that if K is field and $q(x) \in K[x]$ an irreducible polynomial such that $q'(x) \neq 0$, then $q(x)$ had no repeated roots. Prove a slightly more general version of this result : show that $f(x) \in K[x]$ has no repeated roots if and only if $\gcd(f(x), f'(x)) = 1$.

Solution. If $\gcd(f(x), f'(x)) = 1$ then there exist $u(x), v(x) \in K[x]$ such that

$$u(x)f(x) + v(x)f'(x) = 1.$$

Let α be any root of $f(x)$. In class we have seen that if α is a root of $f(x)$ of multiplicity 2 or more, then α is also a root of $f'(x)$. Plugging $x = \alpha$ into the equation above gives us

$$1 = u(\alpha)f(\alpha) + v(\alpha)f'(\alpha) = u(\alpha) \cdot 0 + v(\alpha)f'(\alpha) = v(\alpha)f'(\alpha)$$

from which we conclude that $f'(\alpha) \neq 0$, and therefore that α is not a repeated root of $f(x)$. Therefore we have shown that if $\gcd(f(x), f'(x)) = 1$ then $f(x)$ has no repeated roots.

Now suppose that α is a root of $f(x)$ of multiplicity one. Then we can write $f(x) = (x - \alpha)g(x)$ with $g(\alpha) \neq 0$. Taking the derivative gives

$$f'(x) = g(x) + (x - \alpha)g'(x),$$

and plugging $x = \alpha$ into this we compute that

$$f'(\alpha) = g(\alpha) + 0 \cdot g'(\alpha) = g(\alpha) \neq 0.$$

In other words, if α is a root of $f(x)$ of multiplicity one then α is not a root of $f'(x)$. Thus, if all roots of $f(x)$ have multiplicity one then $f(x)$ and $f'(x)$ have no roots in common.

Let $h(x) = \gcd(f(x), f'(x))$. Since $h(x)$ divides both $f(x)$ and $f'(x)$, any root of $h(x)$ is a common root of $f(x)$ and $f'(x)$. If $f(x)$ has no repeated roots, then as we have seen above, $f(x)$ and $f'(x)$ have no roots in common, and therefore $h(x)$ is a polynomial with no roots. Since $h(x)$ has no roots (in any field) we conclude that $h(x)$ is a constant polynomial. Since the gcd is always monic, this means that $1 = h(x) = \gcd(f(x), f'(x))$. $\square$

5. For each of the following polynomials f_i, let L_i be the field generated by $\mathbb{Q}$ and all the roots of f_i. That is, if $\alpha_1, \ldots, \alpha_r$ are the roots of f_i, let $L_i = \mathbb{Q}(\alpha_1, \ldots, \alpha_s)$. (In other words, L_i is the *splitting field* of each f_i.) In each case find all the roots of f_i, and find the degree of L_i over $\mathbb{Q}$.

(a) $f_1 = x^4 - 5x^2 + 6$.

(b) $f_2 = x^3 - 1$.

(c) $f_3 = x^6 - 1$.

(d) $f_4 = x^6 - 2$.

Solution.

(a) The polynomial $f_1(x)$ is reducible over $\mathbb{Q}$: $f_1(x) = (x^2 - 2) \cdot (x^2 - 3)$ with roots $\pm\sqrt{2}$, $\pm\sqrt{3}$. The splitting field of f_1 over $\mathbb{Q}$ is therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. In previous homework questions (**H1** Q3 and **H2** Q3) we have seen that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

(b) We have $f_2(x) = (x-1)(x^2+x+1)$ with roots 1, ω, and ω^2, where $\omega = e^{2\pi i/3}$. The splitting field for f_2 over $\mathbb{Q}$ is therefore $\mathbb{Q}(1, \omega, \omega^2) = \mathbb{Q}(\omega)$. In **H3** Q3 we have shown that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, and that $q(x) = x^2 + x + 1$ is the minimal polynomial for ω.

(c) The roots of f_3 are the sixth roots of unity : ± 1, $\pm\omega$, and $\pm\omega^2$, where $\omega = e^{2\pi i/3}$ just as in part (b). Therefore the splitting field of $f_3(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\pm 1, \pm\omega, \pm\omega^2) = \mathbb{Q}(\omega)$. I.e., the splitting field for $f_3(x)$ is the same as the splitting field for $f_2(x)$. Of course, we again have $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

(d) The roots of $f_4(x)$ are the sixth roots of 2: $\pm\sqrt[6]{2}$, $\pm\sqrt[6]{2}\omega$, $\pm\sqrt[6]{2}\omega^2$, and the splitting field of $f_4(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\pm\sqrt[6]{2}, \pm\sqrt[6]{2}\omega, \pm\sqrt[6]{2}\omega^2) = \mathbb{Q}(\sqrt[6]{2}, \omega)$.

To compute the degree of $\mathbb{Q}(\sqrt[6]{2}, \omega)$ over $\mathbb{Q}$, we analyze the extension in two steps. By Eisenstein's criterion with $p = 2$, the polynomial $f_4(x)$ is irreducible over $\mathbb{Q}$, and therefore $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = \deg(f_4(x)) = 6$. We know the minimal polynomial of ω over $\mathbb{Q}$ is $q(x) = x^2 + x + 1$ of degree 2. Let $q_M(x)$ be the minimal polynomial of ω over $M = \mathbb{Q}(\sqrt[6]{2})$. We know that $q_M(x)$ divides $q(x)$ and therefore $q_M(x)$ has degree 1 or 2. But $q_M(x)$ has degree 1 if and only if $\omega \in M$. But since $M \subset \mathbb{R}$, and since $\omega \notin \mathbb{R}$, this can't happen. Thus the degree of $q_M(x)$ is 2, and $[\mathbb{Q}(\sqrt[6]{2}, \omega) : \mathbb{Q}(\sqrt[6]{2})] = 2$. We therefore conclude that

$$[\mathbb{Q}(\sqrt[6]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}, \omega) : \mathbb{Q}(\sqrt[6]{2})] \cdot [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 2 \cdot 6 = 12.$$