**Problem 1.** *Show that an angle of* $30^\circ$ *and an angle of* $15^\circ$ *cannot be trisected.*

*Proof.* First note that if $15^\circ$ can be trisected then so can $30^\circ$ as we could bisect $30^\circ$, trisect $15^\circ$ and then double the resulting angle. As such it will suffice to show that we cannot trisect $15^\circ$.

A number is constructible if, and only if, both its real and imaginary parts are constructible. If $15^\circ$ were constructible then so would $e^{i\cdot 10^\circ}$ as it would be the intersection of the angle and the unit circle. The real part of which is

$$\alpha = \cos 10^\circ = \frac{1}{2}\sqrt{\frac{1}{2}\left(4 + 2\cdot\left(\frac{1}{2}(1+i\sqrt{3})^{-\frac{1}{3}} + 2^{\frac{2}{3}}(1+i\sqrt{3})\right)\right)}$$

We know that a number is constructible if, and only if, we have an ascending chain of fields $\mathbb{Q} = F_0 \subset \cdots \subset F_n = \mathbb{Q}[\alpha]$ where all of the intermediate degrees are two. This enforces that the degree of the extension must be a power of 2. However for $\alpha$ at some point we will have to adjoin $(1+i\sqrt{3})^{-\frac{1}{3}}$ for which the extension will be of degree 3. By the tower theorem this means that $3|\mathbb{Q}[\alpha]$ but this cannot occur.

Therefore $\alpha$ is not constructible and it then follows that neither $15^\circ$ nor $30^\circ$ can be trisected. □

**Problem 2.** *Let* $\xi = e^{2\pi i/6} = \cos(2\pi/6) + i\sin(2\pi/6)$ *be a primitive* $6^{th}$ *root of unity over* $\mathbb{Q}$. *Find each of the following:*

1. *The minimum polynomial* $f(x) \in \mathbb{Q}[x]$ *of* $\xi$ *over* $\mathbb{Q}$.
2. *The splitting field* $F$ *of* $f(x)$ *over* $\mathbb{Q}$.
3. $[F : \mathbb{Q}]$.

(a) Let $f(x) = x^2 - x + 1$. This polynomial has $\xi$ as a root. Moreover it is irreducible by the rational roots theorem as $\pm 1$ are not roots.

(b) The roots of $f$ are $\xi$ and $-e^{2\pi i/3} = -\xi^2$. Thus $\mathbb{Q}[\xi, -\xi^2] = \mathbb{Q}[\xi]$ is the splitting field for $f$.

(c) Since the degree of $f$ is 2 it follows that $[\mathbb{Q}[\xi] : \mathbb{Q}] = 2$.

**Problem 3.** *Find a splitting field extension* $K : \mathbb{Q}$ *for each of the following polynomials over* $\mathbb{Q}$ *and in each case determine the degree* $[K : \mathbb{Q}]$.

$$(a)\ x^4+1 \qquad (b)\ x^4+4 \qquad (c)\ (x^4+1)(x^4+4) \qquad (d)\ (x^4-1)(x^4+4)$$

(a) The roots of $f(x) = x^4 + 1$ are $r := e^{\pi i/4}, r^3, r^5$, and $r^7$. Since each all of the other roots can be expressed as a power of $r$ we have that the splitting field of $f$ is $\mathbb{Q}[r, r^3, r^5, r^7] = \mathbb{Q}[r]$ the degree of which is 4 as $f$ is irreducible and thus the minimal polynomial. The irreducibility can be checked by shifting to $f(x+1)$ and apply Eisenstein's Criterion with $p = 2$.

(b) The roots of $g(x) = x^4 + 4$ are the same roots as above but with each multiplied by $\sqrt{2}$. Let $s := \sqrt{2}e^{\pi i/4}$. Then the other roots are $s^3/2, s^5/4$, and $s^7/8$. Similar to before the splitting field is then $\mathbb{Q}[s]$ and since this polynomial is irreducible we have that $[\mathbb{Q}[s] : s] = 4$.

(c) The roots of $p(x) = fg(x) = (x^4+1)(x^4+4)$ are the roots of both part $a$ and $b$. Since the roots here are cyclic if we take $rs$ we get $\sqrt{2}e^{\pi i/2}$. Keep multiplying that by $r$ and we can hit every root. Thus the splitting field will be $\mathbb{Q}[r]$ and the minimal polynomial will be the one from part $(a)$ giving us that $[\mathbb{Q}[r] : \mathbb{Q}] = 4$ for the degree of our splitting field.

(d) The roots of $q(x) = (x^4 - 1)(x^4 + 4)$ are the roots of part $b$ as well as $\pm 1$ and $\pm i$. However $s^2/2 = i$ which means that we can express all of the roots in terms of $s$. Similar to part $(c)$ our splitting field is the same as $b$, $\mathbb{Q}[s]$. As before the degree of this splitting field is 4.

**Problem 4.** *Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of $\alpha = \sqrt{2 + \sqrt{2}}$.*

1. *Show that $f(x) = x^4 - 4x^2 + 2$. Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.*
2. *Show that $\mathbb{Q}(\alpha)$ is the splitting field of $f(x)$ over $\mathbb{Q}$.*

(a) It will follow that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ if $f(x) = x^4 - 4x^2 + 2$ is irreducible since $f(\alpha) = 0$. However $f$ is irreducible by Eisenstein's criterion using 2.

(b) The roots of $f$ are $\pm\sqrt{2 \pm \sqrt{2}}$. With

**Problem 5.** *Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field with $p$ elements, where $p$ is a prime number. Write down all monic cubic polynomials in $\mathbb{F}_2[x]$, factor them completely into irreducible factors and construct a splitting field for each of them. Which of these fields are isomorphic?*

1. $(x^3 + x^2 + 1)$ This polynomial is irreducible. The splitting field will be $\mathbb{F}_2/(x^3 + x^2 + 1)$.
2. $(x^3 + x + 1)$ This polynomial is irreducible. The splitting field will be $\mathbb{F}_2/(x^3 + x + 1)$.
3. $(x^3 + x^2 + x + 1)$ This polynomial is equal to $(x + 1)^3$. Since all of its roots are in $\mathbb{F}_2$ its splitting field is $\mathbb{F}_2$.
4. $(x^3+1)$ This polynomial is equal to $(x+1)(x^2+x+1)$. The splitting field will be $\mathbb{F}_2/(x^2+x+1)$.
5. $(x^3 + x^2)$ This polynomial is equal to $x^2(x + 1)$. Since all of its roots are in $\mathbb{F}_2$ its splitting field is $\mathbb{F}_2$.
6. $(x^3 + x)$ This polynomial is equal to $x(x + 1)^2$. Since all of its roots are in $\mathbb{F}_2$ its splitting field is $\mathbb{F}_2$.
7. $(x^3+x^2+x)$ This polynomial is equal to $x(x^2+x+1)$. The splitting field will be $\mathbb{F}_2/(x^2+x+1)$.
8. $(x^3)$ This polynomial is already factored. Since all of its roots are in $\mathbb{F}_2$ its splitting field is $\mathbb{F}_2$.

The ones polynomials with isomorphic splitting fields are $(3, 5, 6, 8)$, $(4, 7)$, and $(1, 2)$. The splitting fields for 4 and 7 are isomorphic as they the same construction. However 1 and 2 are isomorphic since finite fields of the same size are isomorphic.

**Problem 6.** *Let $f(x) = x^3 + 2x + 2 \in \mathbb{F}_3[x]$.*

1. *Show that $f(x)$ is irreducible in $\mathbb{F}_3[x]$.*
2. *Let $\alpha$ be a root of $f(x)$ in some extension field $K$ of $\mathbb{F}_3$, so that $[\mathbb{F}_3[\alpha] : \mathbb{F}_3] = \deg f(x) = 3$. Show that $\mathbb{F}_3[\alpha]$ is a splitting field of $f(x)$ over $\mathbb{F}_3$.*

1. Since $f(0) = -1, f(1) = -1$, and $f(-1) = -1$ this third degree polynomial has no roots and as such is irreducible.

2. Let $K = F[x]/f$. Then let $\alpha := x + \langle f \rangle$.

**Problem 7.** *Suppose that $f(x) \in F[x]$ is irreducible of degree $n > 0$, and let $L$ be the splitting field of $f(x)$ over $F$.*

1. *Suppose that $[L : F] = n!$. Prove that $f(x)$ is irreducible.*
2. *Show that the converse of part (a) is false.*

*Proof.* □