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

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

A number is constructible if, and only if, both its real and imaginary parts are constructible. If $15°$ 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

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

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 α 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 α is not constructible and it then follows that neither $15°$ nor $30°$ can be trisected. $\square$

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* ξ *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 ξ as a root. Moreover it is irreducible by the rational roots theorem as ± 1 are not roots.

(b) The roots of f are ξ 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) $x^4 + 1$ *(b)* $x^4 + 4$ *(c)* $(x^4 + 1)(x^4 + 4)$ *(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 $\mathbb{Q}[s]$ this polynomial is $(x^2 + 2x + 1)(x^2 - 2x + 1)$ so we have that $x^2 + 2x + 1$ $[\mathbb{Q}[s] : s] = 2$.

(c) The roots of $p(x) = fg(x) = (x^4 + 1)(x^4 + 4)$ are the roots of both part a and b. Start with r. Not that $r^2 = i$ and that $s = 1 + i$. As such using r we can reach s. Thus adjoining r will give us the splitting field for $p(x)$. 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 ± 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 2.

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 $\pm\sqrt{2 \pm \sqrt{2}}$. Then each of the roots in terms of α will be:

- $-\alpha = -\sqrt{2+\sqrt{2}}$
- $\alpha^3 - 3\alpha = \sqrt{2-\sqrt{2}}$
- $-\alpha^3 + 3\alpha = -\sqrt{2-\sqrt{2}}$

Since all of the roots are in $\mathbb{Q}[\alpha]$ we have that $\mathbb{Q}[\alpha]$ is the splitting field.

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 $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$. The roots are x, x^2, and $x^2 + x + 1$.
2. $(x^3 + x + 1)$ This polynomial is irreducible. The splitting field will be $\mathbb{F}_2[x]/(x^3 + x + 1)$. The roots are $x, x^2, x^2 + x$.
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 $\mathbb{F}_2[x]/(x^2 + x + 1)$.
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 $\mathbb{F}_2[x]/(x^2 + x + 1)$.
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 since splitting are unique and the roots of $(x^3 + x^2 + 1)$ in $F[x]/x^3 + x + 1$ are $x + 1, x^2 + 1$, and $x^2 + x + 1$.

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 α 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 $\alpha := x + \langle f \rangle$. This will be a root of f in K. Then the other roots are $\alpha - 1$ and $\alpha + 1$. To check this if we evaluate

$$f(\alpha - 1) = (\alpha - 1)^3 + 2(\alpha - 1) + 2 = \alpha^3 + 2\alpha + 1 = 0$$

and similarly

$$f(\alpha + 1) = (\alpha + 1)^3 + 2(\alpha + 1) + 2 = \alpha^3 + 2\alpha + 1 = 0$$

Since all of the roots can be obtained from α it follows that $\mathbb{F}_3[\alpha]$ is the splitting field for $f(x)$.

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. Let $f(x)$ be a polynomial of degree n and suppose that f is reducible. Then $f = gh$, where $\deg g = a$ and $\deg h = b$, with $0 < a, b < n$. Let L be the splitting field of f and let L' be the splitting field of g. Then by the tower theorem we have that $[L : F] = [L : L'][L' : F]$. We know that $[L : L'][L' : F] \leq (n - a)!n!$ from a proposition from class. However

$$\binom{n}{a} = \frac{n!}{(n-a)!n!} > 1$$

as $0 < a < n$. Thus

$$[L : F] = [L : L'][L' : F] \leq (n - a)!n! < n!$$

$\square$

Let $f(x) = x^4 + 1$ from above. This polynomial is irreducible however the degree of the field extension is 4 rather than 24.