HOMEWORK 2 SOLUTIONS

See the next page.

1. Problem 1

Let $K = \mathbb{Q}[\alpha]$, where α is a complex root of $x^3 - x - 1$. Now consider $\gamma = 1 + \alpha^2$ over $\mathbb{Q}$.

Since α is a root, we have $\alpha^3 - \alpha - 1 = 0 \Leftrightarrow \alpha^3 = \alpha + 1$

We have;

$$\begin{aligned}
\gamma &= 1 + \alpha^2 \\
\gamma^2 &= 1 + 2\alpha^2 + \alpha^4 \\
&= 1 + 2\alpha^2 + \alpha(\alpha^3) \\
&= 1 + 2\alpha^2 + \alpha^2 + \alpha \\
\gamma^2 &= 1 + \alpha + 3\alpha^2
\end{aligned}$$

Plugging in γ into $x^3 - x - 1$ shows that it isn't a root of this equation. For the irreducible polynomial for γ over $\mathbb{Q}$ to be a quadratic, then we must have $a\gamma^2 + b\gamma + c = 0,\ a, b, c \in \mathbb{Q}$;

$$\begin{aligned}
a\gamma^2 + b\gamma + c &= 0 \\
a(3\alpha^2 + \alpha + 1) + b(\alpha^2 + a) + c &= 0 \\
(3a + b)\alpha^2 + a\alpha + (a + b + c) &= 0 \\
\implies a = b = c &= 0
\end{aligned}$$

Thus, γ must have an irreducible polynomial of at least degree 3. We have $\gamma^3 = \gamma\gamma^2 = 2 + 5\alpha + 7\alpha^2$. Since $1, \gamma, \gamma^2$ are linearly independent over $\mathbb{Q}$, and this is a quadratic, we will be able to find some linear combination that equals γ^3. We have;

$$\begin{aligned}
\gamma^3 &= 7\alpha^2 + 5\alpha + 2 \\
-5\gamma^2 &= -15\alpha^2 - 5\alpha - 5 \\
\hline
&= -8\alpha^2 - 3 \\
+8\gamma - 5 &= 8\alpha^2 + 3 \\
\hline
\gamma^3 - 5\gamma^2 + 8\gamma - 5 &= 0
\end{aligned}$$

We have already shown that no solutions of degree 1 or 2 exists, so this will be irreducible. Thus, $x^3 - 5x^2 + 8x - 5$ will be the minimal polynomial of $\gamma = 1 + \alpha^2$ over $\mathbb{Q}$, where α is a complex root of $x^3 - x - 1$.

2. Problem 2

3. Problem 2 (15.5.2(a))

For this problem, first go through Section 5 (Construction with Ruler and Compass) to understand the proof of the following theorem (converse of what we did in class).

Theorem: Suppose the coordinates of a point p lie in a field $F = F_n$ such that there exists a chain of fields

$$\mathbf{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$$

with $\deg(F_{i+1}/F_i) = 2$ for all i. Then p is constructible by ruler and compass starting with $(0,0)$ and $(0,1)$.

Prove that a regular 5-gon is constructible by ruler and compass. That is, prove that $(\cos(2\pi/5), \sin(2\pi/5))$ is constructible by ruler and compass starting with $(0,0)$ and $(0,1)$.

Firstly, as per workshop 1, we know that $\cos(2\pi/5)$ has degree 2 over $\mathbf{Q}$. Thus, $(\cos(2\pi/5), 0)$ is constructible by ruler and compass. Now consider:

$$\sin(2\pi/5) = \sqrt{1 - \cos(2\pi/5)^2}$$

We know that $1 - \cos(2\pi/5)^2 \in \mathbf{Q}[\cos(2\pi/5)]$. Ergo, $\sin(2\pi/5)$ has degree at most 2 over $\mathbf{Q}[\cos(2\pi/5)]$, and hence $\mathbf{Q}[\cos(2\pi/5)] = \mathbf{Q}[\cos(2\pi/5), \sin(2\pi/5)]$ or $\deg \mathbf{Q}[\cos(2\pi/5), \sin(2\pi/5)]/\mathbf{Q}[\cos(2\pi/5)] = 2$. I.e., $(0, \sin(2\pi/5))$ is also constructible. It follows trivially that $(\cos(2\pi/5), \sin(2\pi/5))$ is constructible by ruler and compass (intersect the lines perpendicular to the horizontal and vertical axes passing through these two points).

3 Question 3

Theorem 3.1. *Suppose $m, n \in \mathbb{Z}$. $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are isomorphic if and only if both $\sqrt{m}$ and $\sqrt{n}$ are in $\mathbb{Q}$ or $\frac{m}{n} = a^2$ for some $a \in \mathbb{Q} \setminus \{0\}$.*

Proof. If $\sqrt{m}$ and $\sqrt{n}$ are in $\mathbb{Q}$, then $\mathbb{Q}[\sqrt{m}] = \mathbb{Q} = \mathbb{Q}[\sqrt{n}]$, so these are isomorphic because they are equal. If instead there exists some $a \in \mathbb{Q}\setminus\{0\}$ such that $\frac{m}{n} = a^2$ then $\sqrt{m} = \pm a\sqrt{n}$, so we have that $\sqrt{m} \in \mathbb{Q}[\sqrt{n}]$ and $\sqrt{n} \in \mathbb{Q}[\sqrt{m}]$. Therefore, we find that $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{n}]$, and thus they are isomorphic via the identity map. Therefore, if $\sqrt{m}, \sqrt{n} \in \mathbb{Q}$ or $\frac{m}{n} = a^2$ for some $a \in \mathbb{Q} \setminus \{0\}$ then $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are isomorphic.

Suppose we have some isomorphism $\phi : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{n}]$. We have that $\phi(1) = 1$, so we find that $\phi(q) = q$ for all rational numbers, so the isomorphism is determined entirely by where it sends $\sqrt{m}$. We have that $\phi(\sqrt{m})^2$ equals $\phi(\sqrt{m}^2) = \phi(m) = m$, so $\phi(\sqrt{m}) = \pm\sqrt{m}$, so ϕ has image $\mathbb{Q}[\sqrt{m}]$. However, by assumption, the image of this isomorphism is $\mathbb{Q}[\sqrt{n}]$ so $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{n}]$.

If $\sqrt{m} \in \mathbb{Q}$, then $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}$, and thus $\mathbb{Q} = \mathbb{Q}[\sqrt{n}]$, so $\sqrt{n} \in \mathbb{Q}$. Similarly, if $\sqrt{n} \in \mathbb{Q}$ then $\sqrt{m} \in \mathbb{Q}$, so they are either both in $\mathbb{Q}$ or both not in $\mathbb{Q}$. If they are both not in $\mathbb{Q}$, then as $\sqrt{n}$ is in $\mathbb{Q}[\sqrt{m}]$ we have some $a, b \in \mathbb{Q}$ such that $\sqrt{n} = a\sqrt{m} + b$ and as $\sqrt{n}$ is not in $\mathbb{Q}$ we have that $a \neq 0$. We thus have that $n = a^2m + 2ab\sqrt{m} + b^2$, which rearranges to tell us that $2ab\sqrt{m}$ is a rational number, and thus $b\sqrt{m}$ is a rational number. This only holds if $b = 0$, so we have that $\sqrt{m} = a\sqrt{n}$ and thus $m = a^2n$, so $\frac{m}{n} = a^2$ for some $a \in \mathbb{Q}$. Therefore, if $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are isomorphic, then either $\sqrt{m}, \sqrt{n} \in \mathbb{Q}$ or $\frac{m}{n} = a^2$ for some $a \in \mathbb{Q} \setminus \{0\}$.

Therefore, $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are isomorphic if and only if both $\sqrt{m}$ and $\sqrt{n}$ are in $\mathbb{Q}$ or $\frac{m}{n} = a^2$ for some $a \in \mathbb{Q} \setminus \{0\}$. $\square$

4. Problem 4

Prove that the subset of $\mathbf{C}$ consisting of the algebraic numbers is algebraically closed.

Proof. Denote the set of algebraic numbers in $\mathbf{C}$ by $\bar{\mathbf{Q}}$. Take a polynomial $f(x)$ of positive degree in $\bar{\mathbf{Q}}[x]$. As $\bar{\mathbf{Q}}[x]$ is a subset of $\mathbf{C}[x]$, we know that $f(x)$ has a root $\alpha \in \mathbf{C}$. Let $f(x) = \sum_{i=0}^{n} a_i x^i$, with each $a_i \in \bar{\mathbf{Q}}$. We then have that α is algebraic over $\mathbf{Q}[a_0, ...a_n]$. We can write the following chain of algebraic extensions:

$$\mathbf{Q} \subset \mathbf{Q}[a_0, ...a_n] \subset \mathbf{Q}[a_0, ...a_n][\alpha]$$

$\mathbf{Q}[a_0, ...a_n]$ is a finite extension of $\mathbf{Q}$, and $\mathbf{Q}[a_0, ...a_n][\alpha]$ is also a finite extension of $\mathbf{Q}[a_0, ...a_n]$. Therefore $\mathbf{Q}[a_0, ...a_n][\alpha]$ is a finite extension of $\mathbf{Q}$ and hence also an algebraic extension. Thus α is algebraic over $\mathbf{Q}$ and any $f(x) \in \bar{\mathbf{Q}}[x]$ has a root in $\bar{\mathbf{Q}}$, so $\bar{\mathbf{Q}}$ is algebraically closed.

$\square$

5 Question 5

Let $f(x) = x^3 + x + 1$ and $g(x) = x^3 + x^2 + 1$ be polynomials in $\mathbb{F}_2[x]$, which are irreducible over $\mathbb{F}_2$. Let $K = \mathbb{F}_2[x]/(f(x))$ and $L = \mathbb{F}_2[y]/(g(y))$.

Theorem 5.1. *There are 3 isomorphisms from K to L, given by mapping x to $y+1$, y^2+1, and y^2+y respectively.*

Proof. As shown in lectures, a field isomorphism $K \to L$ must take $\mathbb{F}_2$ to itself, and must take $x \in K$ to a root of f in L, and then it is fully determined for all other elements of K by the fact it is a ring isomorphism. We also have that every polynomial of degree n factors completely in a field of size p^n, so the cubic f factors in L, as L has size $8 = 2^3$. Therefore, we have a field isomorphism for each of the 3 roots of f in L, so we have 3 isomorphisms $K \to L$.

We can see that $y + 1$ satisfies the cubic $f(y + 1) = 0$ in L as follows.

$$\begin{aligned}
(y+1)^3 + (y+1) + 1 &= y^3 + 3y^2 + 3y + 1 + y + 1 + 1 \\
&= y^3 + 3y^2 + 4y + 3 \\
&= y^3 + y^2 + 1 \\
&= 0
\end{aligned}$$

As also shown in lectures, all the other roots of f in L can be found from one root by applying the Frobenius map, which in this case is given by $\alpha \mapsto \alpha^2$. We thus have that $(y+1)^2$ and $(y+1)^4$ are the other two roots of f. The second root simplifies to y^2+1, and the third root simplifies to y^4+1 which equals $y(y^2+1)+1 = y^3+y+1$ which in turn equals $(y^2+1)+y+1 = y^2+y$. Therefore, the three roots of f in L are given by $y+1$, y^2+1, and y^2+y.

The three isomorphisms $K \to L$ are thus given by mapping x to $y+1$, mapping x to y^2+1, and mapping x to y^2+y.

$\square$