Math 395

Homework 6
Due: 3/28/2024

Name: Avinash Iyer

Collaborators: Antonio Cabello, Nora Manukyan, Nate Hall

Problem 2

We will show that $\{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$ is linearly independent.

Suppose $a + b\sqrt{5} + c\sqrt{7} + d\sqrt{35} = 0$. Then,

$$\left(a + d\sqrt{35}\right)^2 = \left(b\sqrt{5} + c\sqrt{7}\right)^2$$
$$a^2 + 35d^2 - 5b^2 - 7c^2 = 2\sqrt{35}\left(bc - ad\right).$$

Since $2\sqrt{35} \notin \mathbb{Q}$ and $a, b, c, d \in \mathbb{Q}$, this equation is only true if $bc - ad = 0$, so $bc = ad$.

Case 1: Suppose $d = 0$ and $a = 0$. Then,

$$7c^2 + 5b^2 = 0,$$

which is only true if $b = c = 0$.

Case 2: Suppose $d = 0$ and a is not necessarily equal to 0. Then, it must be the case that either b or c is equal to 0.

If $b = c = 0$, then we have $a^2 = 0$, so $a = 0$.

If $b = 0$ with c not necessarily equal to 0, we have

$$a^2 - 7c^2 = 0$$
$$(a - c\sqrt{7})(a + c\sqrt{7}) = 0,$$

meaning $a = c\sqrt{7}$ or $a = -c\sqrt{7}$. Since $a \in \mathbb{Q}$ and $c\sqrt{7} \notin \mathbb{Q}$, this can only be the case if $a = c = 0$.

If $c = 0$ with b not necessarily equal to 0, we have

$$a^2 - 5b^2 = 0$$
$$(a - b\sqrt{5})(a + b\sqrt{5}) = 0$$

meaning $a = b\sqrt{5}$ or $a = -b\sqrt{5}$. Since $a \in \mathbb{Q}$ and $b\sqrt{5} \notin \mathbb{Q}$, this can only be the case if $a = b = 0$.

Case 3: Suppose $a = 0$ and d is not necessarily equal to 0. Then, it must be the case that either b or c is equal to 0.

If $b = c = 0$, we have $35d^2 = 0$, so $d = 0$.

If $b = 0$ with c not necessarily equal to 0, we have

$$\begin{aligned} 35d^2 - 7c^2 &= 0 \\ 7(5d^2 - c^2) &= 0 \\ 7(d\sqrt{5} - c)(d\sqrt{5} + c) &= 0 \end{aligned}$$

meaning $d\sqrt{5} = c$ or $-d\sqrt{5} = c$. Since $c \in \mathbb{Q}$ and $d\sqrt{5} \notin \mathbb{Q}$, this can only be the case if $d = c = 0$.

If $c = 0$ with b not necessarily equal to 0, we have

$$\begin{aligned} 35d^2 - 5b^2 &= 0 \\ 5(7d^2 - b^2) &= 0 \\ 5(d\sqrt{7} - b)(d\sqrt{7} + b) &= 0 \end{aligned}$$

meaning $d\sqrt{7} = b$ or $-d\sqrt{7} = b$. Since $b \in \mathbb{Q}$ and $d\sqrt{7} \notin \mathbb{Q}$, this can only be the case if $d = b = 0$.

Case 4: Suppose toward contradiction that $a \neq 0$ and $d \neq 0$. Then, $a = \frac{bc}{d}$. Substituting, we find

$$\begin{aligned} \left(\frac{bc}{d}\right)^2 + 35d^2 - 5b^2 - 7c^2 &= 0 \\ b^2c^2 + 35d^4 - 5b^2d^2 - 7c^2d^2 &= 0 \\ b^2(c^2 - 5d^2) - 7d^2(c^2 - 5d^2) &= 0 \\ (b - d\sqrt{7})(b + d\sqrt{7})(c - d\sqrt{5})(c + d\sqrt{5}) &= 0 \end{aligned}$$

meaning $b = \pm d\sqrt{7}$ or $c = \pm d\sqrt{5}$. Since $d\sqrt{7}, d\sqrt{5} \notin \mathbb{Q}$, and $b, c \in \mathbb{Q}$, this is only the case if $b = d = 0$ or $c = d = 0$, which is a contradiction.

Problem 3

We will show that $\mathbb{Q}(\sqrt{5} + \sqrt{7}) = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.

Clearly, $\mathbb{Q}(\sqrt{5},\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5}+\sqrt{7})$. We need to show that $\sqrt{7}$ and $\sqrt{5}$ can be written as elements of $\mathbb{Q}(\sqrt{5}+\sqrt{7})$. By difference of squares, we have

$$\sqrt{7}-\sqrt{5} = \frac{2}{\left(\sqrt{7}+\sqrt{5}\right)},$$

meaning

$$\begin{aligned}\sqrt{7} &= \frac{\left(\sqrt{7}+\sqrt{5}\right)+\frac{2}{\left(\sqrt{7}+\sqrt{5}\right)}}{2}\\ \sqrt{5} &= \frac{\left(\sqrt{7}+\sqrt{5}\right)-\frac{2}{\left(\sqrt{7}+\sqrt{5}\right)}}{2}\\ \sqrt{35} &= \frac{1}{2}\left(\sqrt{5}+\sqrt{7}\right)^2-12\end{aligned}$$

Thus, $\mathbb{Q}(\sqrt{5}+\sqrt{7}) \subseteq \mathbb{Q}(\sqrt{5},\sqrt{7})$.

Problem 4

Let $F=\mathbb{Q}(\alpha_1,\dots,\alpha_n)$. Suppose $\alpha_i^2 \in \mathbb{Q}$ for all i. We will show that $\sqrt[3]{2} \notin F$.

If $\alpha_i^2 \in \mathbb{Q}$, then $\alpha_i \in \mathbb{Q}$ or $\alpha_i \notin \mathbb{Q}$. If $\alpha_i \in \mathbb{Q}$, then $[\mathbb{Q}(\alpha_i):\mathbb{Q}]=1$, and if $\alpha_i \notin \mathbb{Q}$, then $m_{\alpha_i,\mathbb{Q}}(x)=x^2-\alpha_i^2$ is the unique monic irreducible polynomial over $\mathbb{Q}$, meaning $[\mathbb{Q}(\alpha_i):\mathbb{Q}]=2$. Thus,

$$[\mathbb{Q}(\alpha_1,\dots,\alpha_n):\mathbb{Q}] = [\mathbb{Q}(\alpha_1,\dots,\alpha_n):\mathbb{Q}(\alpha_1,\dots,\alpha_{n-1})][\mathbb{Q}(\alpha_1,\dots,\alpha_{n-1}):\mathbb{Q}],$$

meaning that, inductively, we have that $[\mathbb{Q}(\alpha_1,\dots,\alpha_n):\mathbb{Q}]=2^k$ for some $k\in\mathbb{Z}_{\geq 0}$.

Suppose toward contradiction that $\sqrt[3]{2}\in\mathbb{Q}(\alpha_1,\dots,\alpha_n)$. Then, since $m_{\sqrt[3]{2},\mathbb{Q}}(x)=x^3-2$ (as it is irreducible by the Eisenstein criterion and monic, thus unique), we have that $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. This implies that $3|2^k$ for some $k\in\mathbb{Z}_{\geq 0}$, which is not possible. Thus, $\sqrt[3]{2}\notin\mathbb{Q}(\alpha_1,\dots,\alpha_n)$.

Problem 5

We will show that x^3-2x-2 is irreducible over $\mathbb{Q}$, then compute $(1+\theta)(1+\theta+\theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$ for θ a root.

To start, we see that x^3-2x-2 is a monic polynomial where $p=2$, so by Eisenstein's criterion and Gauss's Lemma, x^3-2x-2 is irreducible over $\mathbb{Q}$. Thus, we have that elements of $\mathbb{Q}[x]/\langle x^3-2x-2\rangle = a\theta^2+b\theta+c$ for $a,b,c\in\mathbb{Q}$.

We have that $\theta^3-2\theta-2=0$. So,

$$\begin{aligned}(1+\theta)(1+\theta+\theta^2) &= 1+2\theta+2\theta^2+\theta^3\\ &= 3+4\theta+2\theta^2 \in \mathbb{Q}(\theta).\end{aligned}$$

To find $\frac{1+\theta}{1+\theta+\theta^2}$, we find $\frac{1}{1+\theta+\theta^2}$ through the Euclidean algorithm and polynomial long division. Since $\gcd(1+x+x^2, x^3-2x-2) = 1$ (as both are irreducible in $\mathbb{Q}[x]$ and neither is a multiple of the other), we have

$$\begin{aligned} x^3 - 2x - 2 &= (1+x+x^2)(x-1) + (-2x-1) \\ 1 + x + x^2 &= (-2x-1)\left(-\frac{1}{2}x - \frac{1}{4}\right) + \frac{3}{4}. \end{aligned}$$

Multiplying backwards, we have

$$\begin{aligned} 1 &= \frac{4}{3}\left(1 + x + x^2 - \left(-\frac{1}{2}x - \frac{1}{4}\right)(-2x-1)\right) \\ &= \frac{4}{3} + \frac{4}{3}x + \frac{4}{3}x^2 - \frac{4}{3}\left(-\frac{1}{2}x - \frac{1}{4}\right)\left(x^3 - 2x - 2 - (x-1)(x^2+x+1)\right) \\ &= \left(\frac{2}{3}x + \frac{1}{3}\right)\left(x^3 - 2x - 2\right) + \left(-\frac{2}{3}x^2 + \frac{1}{3}x + \frac{5}{3}\right)\left(x^2 + x + 1\right). \end{aligned}$$

In particular, by taking θ as a root of $x^3 - 2x - 1$, we have

$$\begin{aligned} 1 &= \left(\frac{2}{3}\theta + \frac{1}{3}\right)\left(\theta^3 - 2\theta - 2\right) + \left(-\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3}\right)\left(\theta^2 + \theta + 1\right) \\ &= \left(-\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3}\right)\left(\theta^2 + \theta + 1\right), \end{aligned}$$

so

$$\frac{1}{1+\theta+\theta^2} = \left(-\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3}\right),$$

so

$$\begin{aligned} \frac{1+\theta}{1+\theta+\theta^2} &= (1+\theta)\left(-\frac{2}{3}\theta^2 + \frac{1}{3}\theta + \frac{5}{3}\right) \\ &= \frac{5}{3} + 2\theta - \frac{1}{3}\theta^2 - \frac{2}{3}\theta^3 \\ &= \frac{5}{3} + 2\theta - \frac{1}{3}\theta^2 - \frac{2}{3}(2\theta + 2) \\ &= \frac{1}{3} + \frac{2}{3}\theta - \frac{1}{3}\theta^2. \end{aligned}$$