M 431: Assignment 14

Nathan Stouffer

Page 200 — Problem 1

Problem. Show that $a = \sqrt{2} - \sqrt{3}$ is algebraic over $\mathbb{Q}$ of degree at most 4 by exhibiting a polynomial $f(x)$ of degree 4 over $\mathbb{Q}$ such that $f(a) = 0$.

Proof. Consider the function $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. We check that $f(a) = 0$:

$$\begin{aligned} f(a) = f(\sqrt{2} - \sqrt{3}) &= (\sqrt{2} - \sqrt{3})^4 - 10(\sqrt{2} - \sqrt{3})^2 + 1 \\ &= (5 - 2\sqrt{6})^2 - 10(5 - 2\sqrt{6}) + 1 \\ &= 25 + 4 * 6 - 20\sqrt{6} - 50 + 20\sqrt{6} + 1 \\ &= 0 + 0 * \sqrt{6} = 0 \end{aligned}$$

□

Field Description

Problem. Give a concrete description of the two fields $\mathbb{Q}[x]/(p(x))$ and $\mathbb{R}[x]/(p(x))$ for $p(x) := x^2 + 2$. This is to say that you should identify them with some subsets of familiar fields, as done in the lecture.

Proof. For $\mathbb{Q}[x]$ we have $\mathbb{Q}[x]/(p(x)) \cong \mathbb{Q}[i\sqrt{2}] := \{-a2 + bi\sqrt{2} \mid a, b \in \mathbb{Q}\}$. This is a subset of $\mathbb{C}$ that is the rational numbers at any rational multiple of $i\sqrt{2}$.

For $\mathbb{R}[x]$ we have $\mathbb{R}[x]/(p(x)) \cong \mathbb{R}[i\sqrt{2}] := \{-x2 + yi\sqrt{2} \mid x, y \in \mathbb{R}\}$. This the entire field $\mathbb{C}$. Given $z = a + ib \in \mathbb{C}$, take $x = -a/2$ and $y = b/\sqrt{2}$.

□

Smallest Containing Field

Problem. Identify the smallest field containing $\mathbb{Q}$ and $2^{1/4}$ and show that it is a four-dimensional vector space over the field of rational numbers $\mathbb{Q}$.

Proof. Consider $(2^{1/4})^k$ for any $k \in \mathbb{N}$. This gives $2^{1/4}, 2^{1/2}, 2^{3/4}, 2$ up to multiples of powers of 2. Thus to contain $2^{1/4}$ we must at least have $F := \{a * 2^{1/4} + b * 2^{1/2} + c * 2^{3/4} + d * 2 \mid a, b, c, d \in \mathbb{Q}\}$. Since this also contains the rationals (by setting $a = b = c = 0$), we are done!

□

Pentagon

Problem. Show that the regular pentagon (inscribed in the unit circle) is constructible by verifying that $x_0 = \sin(72^\circ)$ can be reached by a chain of two quadratic field extensions: $\mathbb{Q} \subset K \subset \mathbb{Q}(x_0)$.

Proof. Sorry Jarek, I couldn't get this one and am running short on time.

□

Reading

Problem. Read the last paragraph on page 212.

Proof. Did it; and found it quite interesting! It seems like the final result discussed in this paragraph can be used to show that there is no general formula for roots of polynomials of degree ≥ 5. I have also heard of Galois Theory being mentioned in cryptography lectures in my computer science classes, so I am interested to see the connections there.

□