MATH 123 SOLUTIONS PROBLEM SET 9

BENJY FIRESTER

1. $\mathbb{Q}(2^{1/3})$

(i) What is a basis for $\mathbb{Q}(2^{1/3})$ over $\mathbb{Q}$.

(ii) Using division of polynomials, find $q(x) \in \mathbb{Z}[x]$ and $r \in \mathbb{Z}$ such that $(x+1)q(x) = (x^3 - 2) + r$.

(iii) Express $\frac{1}{1+3^{1/3}}$ in the form $a + b \cdot 2^{1/3} + c \cdot 2^{2/3}$ for $a, b, c \in \mathbb{Q}$.

Solution. (i) The numbers $1, 2^{1/3}, 2^{2/3}$ are all irrationally related, and therefore independent over $\mathbb{Q}$. Furthermore, we know that the expected dimension is $\deg(x^3 - 2) = 3$, so this is a basis.

(ii) We know that q must be monic, and the product $q(x)(x+1)$ cannot have a quadratic or linear term. Having no quadratic term means $q(x)$ must have $-x$ as its linear term to cancel x^2. This tells us that its constant term must be $+1$ to cancel $-x$. Therefore, we can compute $q(x)$ as $x^2 - x + 1$ and $r = 3$.

(iii) The above shows us that $(1 + 2^{1/3})(2^{2/3} - 2^{1/3} + 1) = 3$ in $\mathbb{Q}(2^{1/3})$. Therefore, we divide by 3 to get that $\frac{1}{1+2^{1/3}} = \frac{1}{3} - \frac{1}{3}2^{1/3} + \frac{1}{3}2^{2/3}$.

$\square$

2. $\mathbb{C}$ as a matrix group

Find a subring A of the ring of matrices $M_2(\mathbb{R})$ such that A is isomorphic to $\mathbb{C}$.

Solution. Let $z = x + iy$ map to $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Observe

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix}$$

which corresponds to $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$ according to the transformation. Therefore, we have proven that this map is a homomorphism with respect to multiplication. It is a bijection that respects addition and the distributive property, so it is a ring isomorphism as desired.

$\square$

3. Splitting field of $\cos(2\pi/7)$

Let $p(x) = x^3 + x^2 - 2x - 1$.

(i) What are the roots of $p(z + 1/z)$?

(ii) Prove that $t = 2\cos(2\pi/7)$ and $s = 2\cos(4\pi/7)$ are roots of $p(x)$.

(iii) Prove that $\mathbb{Q}(t)$ contains s.

Date: April 18, 2023.

(iv) Prove that $\mathbb{Q}(t)$ is the splitting field for $p(x)$.

Solution. (i) Expanding this out yields

$$p(z + 1/z) = z^{-3} + z^{-2} + z^{-1} + 1 + z + z^2 + z^3$$

which multiplying through by z^3 gives

$$p(z) = 0 \iff 1 + z + z^2 + z^3 + z^4 + z^5 + z^6 = 0.$$

We recognize this polynomials as the quotient $\frac{z^7-1}{z-1}$ showing that this is solved by all non-real seventh roots of unity $e^{2k\pi i/7}$ for $k = 1, 2, 3, 4, 5, 6$.

(ii) Let $\zeta = e^{2\pi i/7}$. We see that $t = \zeta + \zeta^{-1}$ and $s = \zeta^2 + \zeta^{-2}$. The above shows that both t and s satisfy p. Furthermore, define $u = \zeta^3 + \zeta^{-3}$ is $2\cos(6\pi/7)$ also satisfies p.

(iii) We can compute

$$s = \zeta^2 + \zeta^{-2} = (\zeta + \zeta^{-1})^2 - 2 = t^2 - 2$$

showing $s \in \mathbb{Q}(t)$. Similarly,

$$u = \zeta^3 + \zeta^{-3} = (\zeta + \zeta^{-1})^3 - 3(\zeta + \zeta^{-1}) = t^3 - 3t$$

so u is also in $\mathbb{Q}(t)$.

(iv) We know that $p(x) = (x - t)(x - s)(x - u)$ since t, s, u are all different (seen via geometry of unit circle), therefore the above shows that p factors completely in $\mathbb{Q}(t)$ and the degree is minimal (i.e. equal to the degree of the polynomial 3, seen because t^4 is computable in terms of lower degree polynomials in t since $\zeta^3 = 1$), showing it is the splitting field.

$\square$

4. Pentagon

Prove that the construction shown in Figure 1 really does produce a regular pentagon.

Solution. We will show that the interior angles are $2\pi/5$ and by symmetry, only show it for $\angle FOC$.

Assume that the radius of the circle is 1, so by the Pythagorean theorem (and the definition of D being the midpoint of the radius), we can compute that $|CD| = \frac{\sqrt{5}}{2}$. Therefore, $|EO| = \frac{\sqrt{5}}{2} - \frac{1}{2}$.
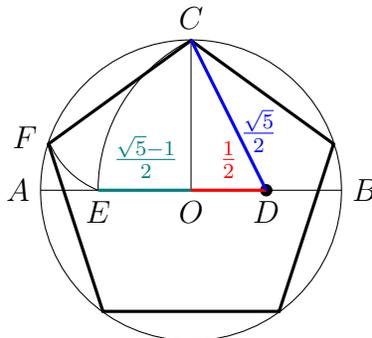
The Pythagorean theorem computes $|CE| = \sqrt{5 - \sqrt{5}}/\sqrt{2}$.[1] This is equal to $|CF|$ since E was formed by the arc centered at C and intersecting F.
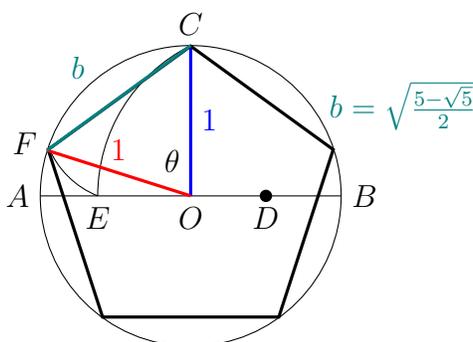
Apply the law of cosines to θ in the picture below to compute

$$\frac{5 - \sqrt{5}}{2} = |OF|^2 + |OC|^2 - 2|OF||OC|\cos(\theta)$$
$$= 1 + 1 - 2\cos(\theta)$$

which we can rearrange to solve for $\cos(\theta)$ as:

$$\cos(\theta) = \frac{\sqrt{5} - 1}{4}$$

which from problem set 5 problem 3 shows that $\theta = \frac{2\pi}{5}$.

Thanks to Quinn Brussel for the Tikz diagrams used here.

$\square$

5. Rational functions in t^2

Let $L = \mathbb{C}(t)$ be the field of rational functions over $\mathbb{C}$, and let $K = \mathbb{C}(t^2) \subset L$ Prove that L is isomorphic to K. What is $[L : K]$?

Solution. Consider the map $L \to K$ given by $t \mapsto t^2$. $\mathbb{C}(t)$ is defined by adding in a variable t satisfying no relations and enforcing that it is a field by adding in all formal inverses. The above map therefore defines a unique ring homomorphism which is bijective by construction (since both are $\mathbb{C}(*)$ are rational functions in a symbol, so we mapped one symbol to another).

We claim that $[L : K] = 2$ with basis $\{1, t\}$. Consider that any polynomial can be decomposed into its even and odd terms, notably its odd terms are all t times an even term. Therefore, the only problem is the denominator might have odd and even terms.

To fix this, we use the fundamental theorem of algebra that $\mathbb{C}$ is algebraically complete. Therefore, $\frac{1}{x-a}$ can be expressed as $\frac{(x+a)}{x^2-a^2}$ which has only even degree terms in the denominator. Therefore, to express any element as a sum of a rational function in t^2 and t times a rational function in t^2, we follow these steps:

- Let $F = \frac{P}{Q}$ with P and Q polynomials in t.

---

[1]This should remind you of problem set 5 which showed that $\sin(\pi/5) = \frac{\sqrt{5-\sqrt{5}}}{2\sqrt{2}}$.

- Rewrite Q by factoring

$$Q = \frac{1}{\prod(x - a_i)} = \prod \frac{(x + a_i)}{x^2 - a_i^2}$$

- Express F equivalently as $\frac{P\prod(x+a_i)}{\prod(x^2-a_i^2)}$, so we can assume without loss of generality that Q is a polynomial in t^2
- Write $P = P_e + P_o$ where P_e is a polynomial in t^2 and P_o is a polynomial with only odd degree terms.
- Express $F = \frac{P_e}{Q} + t\frac{P_o}{Q}$.

$\square$

6. BONUS

Prove that if $p = 2^n + 1$ is prime, and $n > 0$, then n is a power of 2.

Solution. Let $n = 2^a b$ for b odd. Let $p(x) = x^n + 1$ and observe that $x + 1$ when n is odd since $x = -1$ evaluates to zero: $(-1)^n + 1$. We can factor

$$p(x) = (x^{2^a} + 1)(x^{2^a(b-1)} - x^{2^a(b-2)} + \cdots - x^{2^a} + 1)$$

which is non-trivial unless $b = 1$, so set $x = 2$ for a factorization.

$\square$