

## WORKSHOP 1

2024 ALGEBRA 2

### 1. DEGREE OF $\mathbf{Q}(\cos(2\pi/p))$ ?

Let  $p$  be a prime number. What is the degree of  $\mathbf{Q}(\cos(2\pi/p))$  over  $\mathbf{Q}$ ?

#### Hints

Use that  $\mathbf{Q}(\cos(2\pi/p) + i \sin(2\pi/p))$  has degree  $(p-1)$  over  $\mathbf{Q}$  and it contains  $\mathbf{Q}(\cos(2\pi/p))$ .

**Solution.** The multiplicative inverse of  $\cos(2\pi/p) + i \sin(2\pi/p)$  is  $\cos(2\pi/p) - i \sin(2\pi/p)$ , and the sum of these two numbers is  $2 \cos(2\pi/p)$ . So we see that  $\cos(2\pi/p) \in \mathbf{Q}(\cos(2\pi/p) + i \sin(2\pi/p))$ . As a result, we have

$$\mathbf{Q}(\cos(2\pi/p)) \subset \mathbf{Q}(\cos(2\pi/p) + i \sin(2\pi/p)).$$

The element  $\cos(2\pi/p) + i \sin(2\pi/p)$  satisfies the degree 2 equation

$$x^2 - 2 \cos(2\pi/p)x + 1$$

over the smaller field, so this is at most a quadratic extension. But it is a non-trivial extension because the bigger field contains non-real numbers. So this extension has degree 2. Using that the bigger field has degree  $(p-1)$  over  $\mathbf{Q}$ , we conclude that the smaller field has degree  $(p-1)/2$  over  $\mathbf{Q}$ .

**Further question** (come back to it later)—

What is the degree of  $\mathbf{Q}(\cos(2\pi/p), \sin(2\pi/p))$  over  $\mathbf{Q}$ ?

**Solution.** It is either the same as the degree of  $\mathbf{Q}(\cos(2\pi/p))$  or twice it, but I am not sure which one.

### 2. MOST ANGLES CANNOT BE TRISECTED

See if you can prove the following theorem.

**Theorem** — Let  $t$  be such that  $\cos t$  is transcendental. Given  $(0, 0)$ ,  $(0, 1)$ , and  $(\cos t, \sin t)$ , it is impossible to construct  $(\cos t/3, \sin t/3)$  using ruler and compass.

#### Sketch of the proof

Follow the same method as in class, keeping track of the field that contains the coordinates of the constructed points. The starting field

will be  $\mathbf{Q}(\cos t, \sin t)$ . The key is to prove that  $\cos(t/3)$  has degree 3 over this field. It is easier to handle the field  $\mathbf{Q}(\cos t)$ , which is isomorphic to  $\mathbf{Q}(x)$ , the field of rational functions in a variable  $x$ . Over this field, prove that  $\cos(t/3)$  has degree 3. To do so, you need to prove that a certain polynomial in  $\mathbf{Q}(x)[y]$  is irreducible. Using the ideas in class, move through irreducibility in  $\mathbf{Q}(x)[y]$ , in  $\mathbf{Q}[x, y]$ , and  $\mathbf{Q}(y)[x]$ . Finally conclude that over  $\mathbf{Q}(\cos(t), \sin(t))$  also  $\cos(t/3)$  must have degree 3.

**Solution.** We follow the same idea as in class. Recall that the starting point is a field  $F$  that contains the coordinates of our points. We cannot start with  $F = \mathbf{Q}$ , but we take  $F$  to be the smallest subfield of  $\mathbf{C}$  containing  $\cos t$  and  $\sin t$ .

How do we describe  $F$ ? It is easier to first look at a smaller field  $G$ , which is the smallest subfield of  $\mathbf{C}$  containing  $\cos t$ . Convince yourselves that

$$G = \{p(\cos t)/q(\cos t) \mid p, q \in \mathbf{Q}[x], q \neq 0\}.$$

Furthermore, the map

$$\mathbf{Q}(x) \rightarrow G$$

that sends  $x \mapsto \cos t$  is an isomorphism.

Now  $F = G[\sin t]$  is at most a quadratic extension of  $G$ . The new element  $\sin t$  satisfies the quadratic polynomial

$$y^2 + \cos^2 t - 1 = 0$$

(This polynomial is in fact irreducible over  $G$ , but we do not need this fact.)

Now, by the triple angle formula,  $\cos(t/3)$  satisfies the equation

$$4y^3 - 3y - \cos t = 0$$

We claim that this is irreducible over  $F$ . It is easier to see that it is irreducible over  $G$ . Indeed, using the isomorphism above, we can rewrite it as  $4y^3 - 3y + x$ . We now switch to  $\mathbf{Q}[x, y] = \mathbf{Q}[y, x]$ , and then to  $\mathbf{Q}(y)[x]$  (why can we do this?) But in the last ring, it is a linear polynomial and hence irreducible.

We conclude that  $\cos(t/3)$  has degree 3 over  $G$ . Then  $G[\sin t, \cos(t/3)]$  has degree 3 or 6 over  $G$ . In either case,  $\cos(t/3)$  must have degree 3 over  $F = G[\sin t]$ .

But then we are done: there is no way to construct  $\cos(t/3)$  starting from  $G$ .