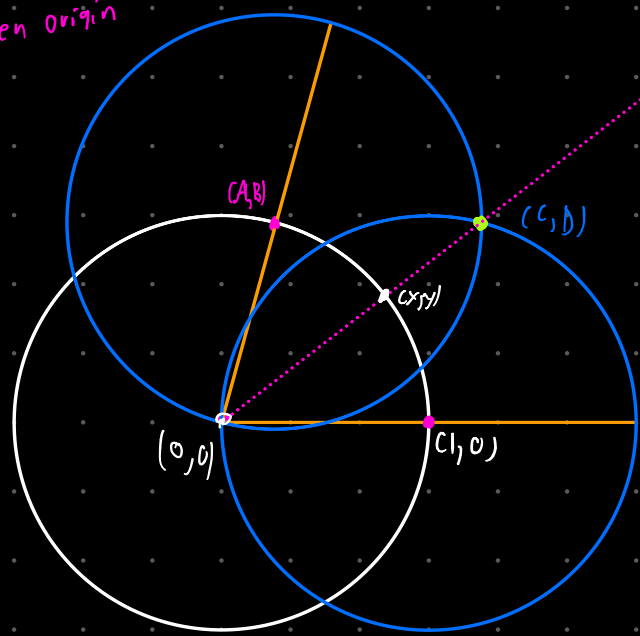
Bisecting Angle

1. Reduce to angle between two points (1,0) and (A,B) on unit circle
2. Draw circles of radius 1 about (A,B) and (1,0), mark off (C,D) intersection
3. Draw line between origin and (C,D), this line bisects the angle



(C, D) on circle radius 1 at (A,B) and circle radius 1 at (1,0)

$$(C-A)^2 + (D-B)^2 = 1 \quad \text{and} \quad (C-1)^2 + D^2 = 1$$

$$(C-A)^2 - (C-1)^2 + (D-B)^2 - D^2 = 0$$

$$\cancel{C^2} - 2AC + A^2 - [\cancel{C^2} - 2C + 1] + \cancel{D^2} - 2DB + B^2 - \cancel{D^2} = 0$$

$$2C - 1 - 2AC - 2DB + \overbrace{A^2 + B^2}^{1} = 0$$

$$2C = 2AC + 2DB$$

$$C = AC + DB$$

$$C(1-A) = DB \quad \text{so} \quad \frac{D}{C} = \frac{1-A}{B} = \frac{Y}{X} \quad x^2+y^2=1$$

want $2xy = B$ $\leftarrow$ From double angle $\sin 2\theta = 2\cos\theta\sin\theta$

$$1 = X^2 + y^2 = X^2 + \left(\frac{1-A}{B}\right)^2 X^2 = X^2\left(1 + \left(\frac{1-A}{B}\right)^2\right) = 1$$

$$\text{So} \quad X^2 = \frac{1}{1+\left(\frac{1-A}{B}\right)^2} = \frac{B^2}{2-2A} = \frac{B^2}{2(1-A)} \quad \text{so} \quad X = \frac{B}{\sqrt{2-2A}} = \frac{B}{\sqrt{2}\sqrt{1-A}}$$

$$1 + \left(\frac{1-A}{B}\right)^2 = \frac{B^2 + 1 + A^2 - 2A}{B^2} = \frac{2-2A}{B^2}$$

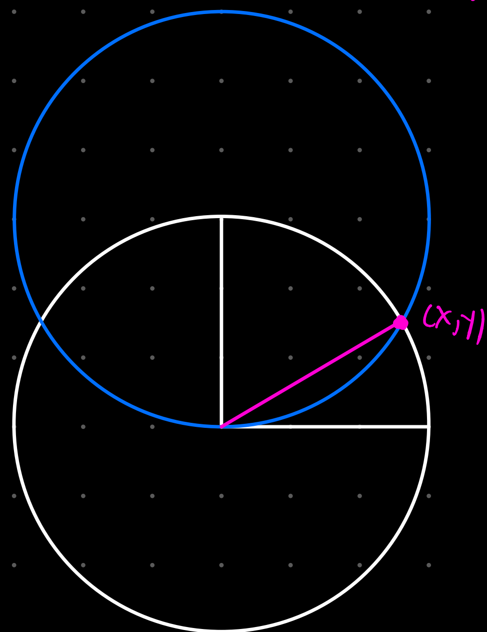
$$\text{So } 2xy = 2x^2\frac{1-A}{B} = 2\left(\frac{1-A}{B}\right)\left(\frac{B^2}{2(1-A)}\right) = B \qquad \square$$

Trisecting 90° angle

① Reduce to angle between (1,0), (0,0) and (0,1), draw unit circle

② Draw circle radius 1 centered at (0,1), mark off intersection (x,y)

③ Draw line between origin and (x,y). This yields the 30° angle



$x^2+y^2=1$ $\quad x^2+(1-y)^2=1$

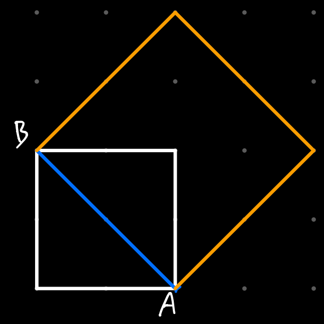
$y^2-(1-y)^2=0$

$y^2-[1+y^2-2y]=0$

so $2y=1$

so $y=\frac{1}{2}$ ✓

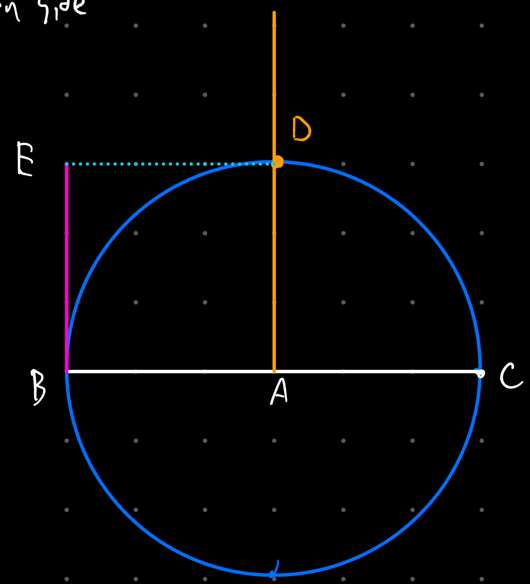
Double the square



1. Start with square
2. Draw diagonal AB
3. Construct square with side AB to finish

(see next page for details on 3)

Draw square given side



① Start with AB

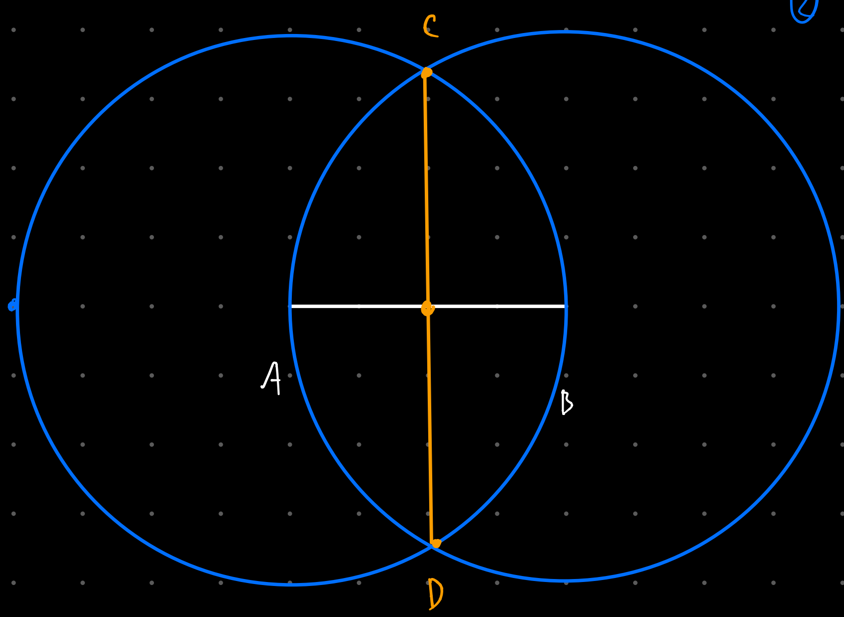
② Draw circle of radius AB, center A, mark off C

③ Draw perpindicular bisector to BC, mark off D

④ Repeat 1, 2, 3 on other side to get BE ≅ AD

⑤ Draw ED to finish (dashed)

Perpindicular bisector



1. Start with AB
2. Draw circles radius AB centers at A and B, mark off C and D
3. Draw CD to finish

Math 404 HW 4 Solutions

1 Problem 5.4

> Let η be a primitive 9th root of unity.
>
> (a) What is the minimal polynomial for η?
>
> (b) Write η^{-1} as a $\mathbb{Q}$-linear combination of $1, \eta, \eta^2, \ldots, \eta^5$.

1. We understand the minimal polynomials for primitive p-th roots of unity where p is a prime, so here we try to relate the study of this 9th root of unity to that of a primitive 3rd root of unity. In particular, note that $(\eta^3)^3 = 1$ and $\eta^3 \neq 1$, so that η^3 is a primitive 3rd root of unity. The last homework yields that η^3 is a root of $f(x) = x^2 + x + 1$. Thus, we have that η is a root of

$$g(x) := f(x^3) = x^6 + x^3 + 1.$$

Then we note that

$$g(x+1) = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$$

which satisfies Eisenstein's criterion at $p = 3$, so is irreducible. Thus, we have that $g(x)$ is irreducible, and so is the minimal polynomial for η.

$\square$

2. We give two solutions. One that is more following your nose, and another that's more abstract.

1.1 Following your nose

Suppose we have a linear combination

$$\eta^{-1} = \sum_{i=0}^{5} a_i \eta^i$$

with $a_i \in \mathbb{Q}$. By definition of multiplicative inverses, this is true if and only if

$$\left(\sum_{i=0}^{5} a_i \eta^{i+1}\right) - 1 = 0.$$

The left hand side of this equation is a polynomial η. By definition of a minimal polynomial, this holds if and only if there is some $h(x) \in \mathbb{Q}[x]$ so that

$$\left(\sum_{i=0}^{5} a_i x^{i+1}\right) - 1 = h(x) \cdot (x^6 + x^3 + 1).$$

Since the left hand side is a nonzero polynomial of degree at most 6, the only possibility is that $h(x)$ is a nonzero constant. Investigating the constant terms on both sides yields that we must have $h(x) = -1$. This yields $a_5 = -1, a_2 = -1,$ and $a_i = 0$ for all other i. That is, we have

$$\eta^{-1} = -\eta^5 - \eta^2.$$

1.2 More abstract

We know by previous work that we have an isomorphism $\varphi : \mathbb{Q}[x]/(g(x)) \xrightarrow{\sim} \mathbb{Q}(\eta)$ defined by sending $x \mapsto \eta$. We also know that the former ring is a $\mathbb{Q}$-vector space with basis $1, x, \ldots, x^5$ (all powers of x smaller than the degree of g). Since $\mathbb{Q}[x]/(g(x))$ is a field, with η identified under this isomorphism with the class of x, we must have that $1/x$ is a linear combination of these x^i. Furthermore, if we actually go back and look at our proof that $\mathbb{Q}[x]/(g(x))$ is a field when g is irreducible, we actually get an algorithm for finding the inverses of elements.

Since g is irreducible and x does not divide g (if it did, then by irreducibility we would have $g = x$ so $\eta = 0$), we must have that the greatest common divisor of g and x is 1. Furthermore, by applying the Euclidean algorithm, we can produce polynomials u and v so that $ug+vx=1$. Then the class of v will be the inverse of x in $\mathbb{Q}[x]/(g(x))$. And we can furthermore find these u and v by just doing repeated division with remainder.

Indeed, by one division with remainder we get

$$g = x^6 + x^3 + 1 = x(x^5 + x^2) + 1.$$

Rearranging gives

$$1 = g + x(-x^5 - x^2).$$

Thus, we have that $-x^5 - x^2 = x^{-1}$ in the quotient ring, and applying φ yields $\eta^{-1} = -\eta^5 - \eta^2$.

$\square$

Exercise *The reasoning above applies much more generally. See if you can carry it out for any field extension $K \subset K(\eta)$, with η algebraic. Let $g(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ be the minimal polynomial for η. Show that $a_0 \neq 0$, and find a formula for $1/\eta$ in terms of the a_i. Furthermore, let $h(x) \in K[x]$ be a nonzero polynomial of degree less than n. Let $\gamma = g(\eta)$. Show abstractly that γ^{-1} can be written as a K-linear combination of η^i, with $0 \leq i \leq n-1$. See if you can use this to find $(1+\eta)^{-1}$ in $\mathbb{Q}(\eta)$ where η is a primitive 9th root of unity.*

2 Problem 5.5

Determine the splitting fields $\mathbb{Q} \subset K$ of each of the following polynomials defined over $\mathbb{Q}$ and compute the degree $|K : \mathbb{Q}|$.

(a) $f(x) = x^3 - 2$.

(b) $f(x) = x^4 - 3$

(c) $f(x) = x^9 - 1$.

(a) Let $\sqrt[3]{2}$ denote the real cube root of 2. Let ω be a primitive cube root of unity. I claim $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, and $|K : \mathbb{Q}| = 6$. For the first claim, note that the other roots of f are $\alpha = \omega\sqrt[3]{2}$ and $\beta = \omega^2\sqrt[3]{2}$. This shows that $\mathbb{Q}(\sqrt[3]{2}, \omega)$ contains all the roots of f, so by minimality we have $K \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$. For the reverse containment, note that K contains $\sqrt[3]{2}$ and α, so K also contains $\alpha/\sqrt[3]{2} = \omega$. Thus, we have $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

For the degree statement, consider the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$. Since f is irreducible over $\mathbb{Q}$ by Eisenstein, the degree of the first field extension is three. For the extension $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$, recall that ω is a root of $g = x^2 + x + 1$. So this extension is of degree either 2 or 1. However, it can not be of degree 1, as $\sqrt[3]{2} \in \mathbb{R}$ so $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ but $\omega \notin \mathbb{R}$. Thus, this extension must be degree 2, and the result holds by the multiplicative property of the degree.

$\square$

(b) Let $\sqrt[4]{3}$ denote the real fourth root of 3. I claim that $K = \mathbb{Q}(\sqrt[4]{3}, i)$, and $|K : \mathbb{Q}| = 8$. For the first claim, note that the roots of f are $\pm\sqrt[4]{3}$ and $\pm i\sqrt[4]{3}$, which shows that all the roots of f are in $\mathbb{Q}(\sqrt[4]{3}, i)$, so $K \subset \mathbb{Q}(\sqrt[4]{3}, i)$. For the reverse containment, note that since K contains all the roots of f, it contains $\sqrt[4]{3}$ and $\frac{i\sqrt[4]{3}}{\sqrt[4]{3}} = i$, so we get $K \supset \mathbb{Q}(\sqrt[4]{3}, i)$, and equality holds.

For the degree statement, consider the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{3}) \subset \mathbb{Q}(\sqrt[4]{3}, i)$. Since f is irreducible over $\mathbb{Q}$ by Eisenstein, the first extension is of degree 4. Since i is a root of $g = x^2 + 1$, we have that the latter extension is of degree at most 2. Since $\sqrt[4]{3} \in \mathbb{R}$, we have that

$\mathbb{Q}(\sqrt[4]{3}) \subset \mathbb{R}$. Since $i \notin \mathbb{R}$, we must have that $\mathbb{Q}(\sqrt[4]{3}) \neq \mathbb{Q}(\sqrt[4]{3}, i)$, and so this extension must be of degree 2. The result holds by the multiplicative property of the degree.

□

(c) Let η be a primitive 9th root of unity. I claim that $K = \mathbb{Q}(\eta)$, and that $|K : \mathbb{Q}| = 6$. The latter statement will follow from the first, as we previously showed that η has a minimal polynomial of degree 6. By definition of primitive roots, the roots of f are the elements η^i for $0 \leq i \leq 8$. This shows that $\mathbb{Q}(\eta)$ contains all the roots of f, so we must have $K \subset \mathbb{Q}(\eta)$. Since η is a root of f, we must have $\eta \in K$ so $\mathbb{Q}(\eta) \subset K$, and the result holds.

3 Problem 5.6

Show that the multiplicative group $\mathbb{F}_{11}^\times$ of nonzero elements is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.

Proof. We have a group homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}_{11}^\times$ sending $1 \mapsto 2$ (the former as a group under addition, and the latter as a group under multiplication). Computing powers of 2 mod 11 yields that φ is surjective. Furthermore we can just see that $\varphi(10) = 1$ and $\varphi(n) \neq 1$ for $0 < n < 10$. This shows that $\ker(\varphi) = 10\mathbb{Z}$, so the first isomorphism theorem yields $\mathbb{F}_{11}^\times \cong \mathbb{Z}/10\mathbb{Z}$. The other possible choices of generators are 8, 7, and 6. $\square$