

PS2

Sasha Redden

January 27, 2026

1. Let F/K be a degree 2 extension.
 - (a) Suppose that the characteristic of K is not 2. Prove that there exists $\delta \in F$ such that $F = K(\delta)$ and $\delta^2 \in K$.
 - (b) Show by example that the conclusion is false if $\text{char } K = 2$.
- (a) F/K degree 2 extension so there exists $\delta \in F$ such that $F = K(\delta) \cong K[x]/\langle m_\delta \rangle$ where m_δ is minimal polynomial of δ in of degree 2. Let $m_\delta = f(x) = x^2 + bx + c$ where $b, c \in K$. $f(\delta) = \delta^2 + b\delta + c = 0$ so $\delta^2 + b\delta = -c \in K$, so either $\delta, (\delta + b) \in K$ or $b = 0$, but $\delta \notin K$ because then $F = K$ and the extension is not of degree 2, so we must have that $b = 0$ and thus $-c = \delta^2 \in K$ as desired.
- (b) Consider $F = \mathbb{F}_2[x]/\langle f \rangle$ where $f = x^2 + x + 1$, this is a degree 2 extension from a field $K = \mathbb{F}_2$ of characteristic 2 such that for $\delta = \bar{x}$, $F = \mathbb{F}_2(\delta)$. $\mathbb{F}_2 = \{0, 1\}$, $0^2 = 0$, $1^2 = 1$ since $\delta \notin \mathbb{F}_2$ then $\delta^2 \notin \mathbb{F}_2$.
2. The purpose of this exercise is to prove that it is possible to construct a regular pentagon with a straight-edge and compass.
 - (a) Prove that it is possible to construct a regular pentagon with straight-edge and compass if and only if $\gamma = \cos(2\pi/5)$ is constructible.
 - (b) Prove that γ is constructible. You may use without proof that $4\gamma^2 + 2\gamma - 1 = 0$.
 - (c) (Optional) Given a straight-edge and compass construction of the regular pentagon.
- (a) $\implies$: Suppose a regular pentagon is constructable, then consider a side of the pentagon with an adjacent side parallel to the x -axis such that their intersection is as the origin, the exterior angle of the pentagon measures so $2\pi/5$ so by intersecting the opposite vertex with a line parallel to the y -axis it will intersect the x -axis at exactly $(\cos(2\pi/5), 0)$. $\Leftarrow$: Suppose $\cos(2\pi/5)$ is constructable, then consider the point $a = (\cos(2\pi/5), 0)$ and a line parallel to the y -axis going through a , now consider a unit circle centered at the origin, let the intersection point of the line and the circle be denoted by b , also note that $b = (\cos(2\pi/5), \sin(2\pi/5))$. Construct a line segment from the origin o to b denoted by $B = \overline{ob}$, this is the first edge of the pentagon. Join o to $c = (-1, 0)$ to form $C = \overline{oc}$, then

$\angle BC = 3\pi/5$ which is the internal angle of a regular pentagon. Construct a unit circle centered at c and a line going through $d = (-1 - \cos(2\pi/5), 0)$ parallel to the y -axis, let $e = (1 - \cos(2\pi/5), \sin(2\pi/5))$ be the intersection point of the circle and the line. Then consider the line going through the mid points of $\overline{oc}$ and $\overline{eb}$ and then using unit circles centered at e and b , mark their intersection with the line to obtain the fifth and final point. If it is possible to construct a regular pentagon with straight-edge and compass, then the a line at the exterior angle $2\pi/5$ is constructable and by intersecting the line with a unit circle centered at the origin you can obtain the point $(\cos(2\pi/5), \sin(2\pi/5))$, so by taking the x component (by constructing a line through the point parallel to the y -axis and recovering the line segment on the x -axis to obtain $(\cos(2\pi/5), 0)$, then $\gamma = \cos(2\pi/5)$.

- (b) Consider the circle $c = (x + 1)^2 + y^2 = 2$ and the line $y = \sqrt{3}x$, the circle is obviously constructable and we can construct $\sqrt{3}$ by first constructing $\sqrt{2}$ using a right angle triangle with adjacent side lengths of 1 to obtain $\sqrt{2}$ as the hypotenuse, and then with another right angle triangle with adjacent sides 1 and $\sqrt{2}$, $\sqrt{3}$ can be obtained as the hypotenuse. The point(s) of intersection of this line and circle are described by $(x + 1)^2 + (\sqrt{3}x)^2 = 2 \implies x^2 + 2x + 1 + 3x^2 = 2 \implies 4x^2 + 2x - 1 = 0$ where γ is a solution.
3. The purpose of this exercise to prove that it not is possible to construct a regular 7-gon by straight-edge and compass.
- (a) Let $\gamma = \cos(2\pi/7)$ and let $\zeta_7 = e^{2\pi i/7}$. Using that $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$, show that $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ cannot be a power of 2.
- (b) Prove that it is impossible to construct a regular 7-gon by straight-edge and compass.
- (a) $\zeta_7 = \cos(2\pi/7) + i \sin(2\pi/7)$ so $\mathbb{Q} \subset \mathbb{Q}(\gamma) \subset \mathbb{Q}(\zeta_7)$ so $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}] = 6$ but since $\mathbb{Q}(\zeta_7) = \mathbb{Q}(\gamma, i \sin(2\pi/7))$ the degree of the extension is 2 and thus $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$.
- (b) Since $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ is not a power of 2, we can deduce that γ is not constructable, and thus we cannot construct $2\pi/7$, the exterior angle for a regular 7-gon, so a regular 7-gon is not constructable by straight edge and compass.
4. Describe the splitting field of the polynomial $x^4 + 2$ over $\mathbb{Q}$. In particular find its degree. The roots of polynomial $x^4 + 2$ are $\pm \sqrt[4]{2}\sqrt{\pm i}$ but $\sqrt{-i} = i\sqrt{i}$ and $\sqrt{i} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ so the splitting field of $x^4 + 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i)$. Using the sequence of inclusions $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$, by Tower theorem: $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$. $\mathbb{Q}(\sqrt[4]{2})$ is a simple extension with minimal polynomial $x^4 - 2$ so its degree over $\mathbb{Q}$ is 4 and by adjoining i we increase the degree by 2 so $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 2 \cdot 4 = 8$.
5. Let $n \in \mathbb{N}$. Let $\zeta_n = e^{2\pi i/n}$. Let $\mu_n = \{z \in \mathbb{C} : z^n = 1\}$
- (a) Prove that μ_n is a subgroup of $\mathbb{C}$ (under multiplication).
- (b) Prove that $\mu_n \cong \mathbb{Z}/n$ (as a group) and that ζ_n is a generator.
- (c) We say that $z \in \mu_n$ is a primitive n -th root of unity if z generates μ_n as a group. Prove that ζ_n^k is a primitive n -th root of unity and only if $(k, n) = 1$ (this notation means that

k, n are relatively prime).

(d) Let

$$\Phi_n(x) = \prod_{1 \leq k < n, (k, n) = 1} x - \zeta_n^k$$

Prove that

$$x^n - 1 = \prod_{d|n} \Phi_d \quad (1)$$

- (e) If p is prime, prove that $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$.
(f) Using (1), find $\Phi_6(x)$.
(g) Using (1), prove that $\Phi_n(x)$ is a monic polynomial with integer coefficients. (In class we will prove it is irreducible and hence is the minimal polynomial of ζ_n .)

(a) Let $\alpha, \beta \in \mu_n$, then

$$(\alpha\beta)^n = \alpha^n \beta^n = 1 \implies \alpha\beta \in \mu_n$$

and identity element $1 \in \mu_n$ is also in μ_n because $1^n = 1$. We have inverses for $\alpha \in \mu_n$, $\alpha^{-1} = \alpha^{n-1} = \alpha \alpha^{n-2} = \alpha^{n-1}$, $\alpha \alpha^{n-1} = \alpha^n = 1$ and $(\alpha^{n-1})^n = (\alpha^n)^{n-1} = 1^{n-1} = 1$ so $\alpha^{-1} \in \mu_n$.

- (b) From class $\mu_n = \{z : z^n = 1\} = \{\zeta_n^k : k = 0, \dots, n-1\}$ so $|\mu_n| = n$ and $\text{ord}(\zeta_n) = n$ so ζ_n is a generator of μ_n .
(c) $\implies$: Assume ζ_n^k is a primitive n -th root of unity, and suppose that $(k, n) \neq 1$. W.L.O.G. assume that $k < n$, otherwise ζ_n^k can be reduced to $\zeta_n^{k'}$ where $k = nq + k'$ such that $0 \leq k' < n$. Since we know they are not coprime, they share a common divisor $d > 1$ such that $d|n, k$ so $n = dq', k = dq''$ for some $q', q'' \in \mathbb{Z} : q' > q'', n = k \cdot \frac{q'}{q''}$ so $(\zeta_n^k)^{q'/q''} = \zeta_n^n = 1$ then the order of ζ_n^k is the floor of $q'/q'' < n$, thus it is not a generator of μ_n .
 $\Leftarrow$: Assume $(k, n) = 1$ and again suppose $k < n$. Suppose ζ_n^k is not a primitive n -th root of unity, then ζ_n^k has degree m strictly less than n . Then $(\zeta_n^k)^m = 1$, so $n|km$ but since n and m are coprime, $n|m$, but this is a contradiction because we assumed that m was strictly less than n , thus ζ_n^k is a primitive n -th root of unity.
(d) Consider μ_n , for d such that $d|n$, then ζ_d generates a subgroup $\mu_d \subset \mu_n$, so μ_n can be partitioned into its divisor subgroups where in each subgroup $(\zeta_d^m)^d = 1$ iff $(d, m) = 1$, so the roots of $x^d - 1$ are the roots of $\Phi_d(x)$, so for $x^n - 1$, it follows that the roots are all of the roots of these $\Phi_d(x)$, thus $x^n - 1 = \prod_{d|n} \Phi_d$.
(e) If p is prime then $x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\prod_{1 \leq k < p} x - \zeta_p^k$ so $\Phi_p(x) = x^p - 1 / x - 1$ and using polynomial long division we obtain $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$
(f) $\Phi_6 = (x-1)(x-\zeta_2)(x-\zeta_3)(x-\zeta_3^2)(x-\zeta_6)(x-\zeta_6^5)$
(g) From part d it follows that $\Phi_n(x)$ is monic (all of the factors are monic)...