Great Big Galois Example

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac

- Introduction
- Polynomials and Fundamental Theorem of Algebra
- Visualizing Complex Numbers
- Permuting Roots
- Fixed Fields and Groups

Introduction

- Quadratic Equations (Area) $\sim$ 2000 BCE

Introduction

- Quadratic Equations (Area) $\sim$ 2000 BCE
- Cubic and Quartic Equations $\sim$ 1500 CE

Introduction

- Quadratic Equations (Area) $\sim$ 2000 BCE
- Cubic and Quartic Equations $\sim$ 1500 CE
- Quintic Equations and Above $\sim$ 1800 CE

Introduction

- Quadratic Equations (Area) $\sim$ 2000 BCE
- Cubic and Quartic Equations $\sim$ 1500 CE
- Quintic Equations and Above $\sim$ 1800 CE
- Permutations of Roots and the Birth of Group Theory

- Introduction
- Polynomials and Fundamental Theorem of Algebra
- Visualizing Complex Numbers
- Permuting Roots
- Fixed Fields and Groups

Fundamental Theorem of Algebra

Fundamental Theorem of Algebra: If $f(x)$ is a polynomial of degree n with complex coefficients, then over the complex numbers $f(x)$ factors into a product of n factors, not necessarily all distinct.

Fundamental Theorem of Algebra (Examples)

Consider:

$$3x^4 + 5x^3 - 5x^2 - 5x + 2 =$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$3x^4 + 5x^3 - 5x^2 - 5x + 2 = (x - 1)(3x^3 + 8x^2 + 3x - 2)$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} 3x^4 + 5x^3 - 5x^2 - 5x + 2 &= (x-1)(3x^3 + 8x^2 + 3x - 2) \\ &= (x-1)(x+1)(3x^2 + 5x - 2) \end{aligned}$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} 3x^4 + 5x^3 - 5x^2 - 5x + 2 &= (x-1)(3x^3 + 8x^2 + 3x - 2) \\ &= (x-1)(x+1)(3x^2 + 5x - 2) \\ &= (x-1)(x+1)(x+2)(3x-1) \end{aligned}$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} 3x^4 + 5x^3 - 5x^2 - 5x + 2 &= (x-1)(3x^3 + 8x^2 + 3x - 2) \\ &= (x-1)(x+1)(3x^2 + 5x - 2) \\ &= (x-1)(x+1)(x+2)(3x-1) \\ &= 3(x-1)(x+1)(x+2)(x-1/3) \end{aligned}$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} 3x^4 + 5x^3 - 5x^2 - 5x + 2 &= (x-1)(3x^3 + 8x^2 + 3x - 2) \\ &= (x-1)(x+1)(3x^2 + 5x - 2) \\ &= (x-1)(x+1)(x+2)(3x-1) \\ &= 3(x-1)(x+1)(x+2)(x-1/3) \end{aligned}$$

So, this could be factored using just integers/rationals

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^4 - 12x^2 + 27 =$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^4 - 12x^2 + 27 = (x^2 - 9)(x^2 - 3)$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} x^4 - 12x^2 + 27 &= (x^2 - 9)(x^2 - 3) \\ &= (x - 3)(x + 3)(x^2 - 3) \end{aligned}$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} x^4 - 12x^2 + 27 &= (x^2 - 9)(x^2 - 3) \\ &= (x - 3)(x + 3)(x^2 - 3) \\ &= (x - 3)(x + 3)(x - \sqrt{3})(x + \sqrt{3}) \end{aligned}$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} x^4 - 12x^2 + 27 &= (x^2 - 9)(x^2 - 3) \\ &= (x - 3)(x + 3)(x^2 - 3) \\ &= (x - 3)(x + 3)(x - \sqrt{3})(x + \sqrt{3}) \end{aligned}$$

This could be partially factored using integers, but required real numbers to finish the job

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^4 - 9 =$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^4 - 9 = (x^2 - 3)(x^2 + 3)$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} x^4 - 9 &= (x^2 - 3)(x^2 + 3) \\ &= (x - \sqrt{3})(x + \sqrt{3})(x^2 + 3) \end{aligned}$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} x^4 - 9 &= (x^2 - 3)(x^2 + 3) \\ &= (x - \sqrt{3})(x + \sqrt{3})(x^2 + 3) \\ &= (x - \sqrt{3})(x + \sqrt{3})(x - i\sqrt{3})(x + i\sqrt{3}) \end{aligned}$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$\begin{aligned} x^4 - 9 &= (x^2 - 3)(x^2 + 3) \\ &= (x - \sqrt{3})(x + \sqrt{3})(x^2 + 3) \\ &= (x - \sqrt{3})(x + \sqrt{3})(x - i\sqrt{3})(x + i\sqrt{3}) \end{aligned}$$

This could be partially factored using integers and reals, but required imaginary numbers to factor it completely. Note that when the coefficients of the polynomial are real, any complex roots come in *conjugate pairs*.

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^3 - 2 =$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^3 - 2 = (x - \sqrt[3]{2})\left(x^2 + x\sqrt[3]{2} + \sqrt[3]{2}^2\right)$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^3 - 2 = (x - \sqrt[3]{2})\left(x^2 + x\sqrt[3]{2} + \sqrt[3]{2}^2\right)$$
$$= (x - \sqrt[3]{2})\left(x - \left(\frac{1 + i\sqrt{3}}{2}\right)\sqrt[3]{2}\right)\left(x - \left(\frac{1 - i\sqrt{3}}{2}\right)\sqrt[3]{2}\right)$$

Fundamental Theorem of Algebra (Examples)

Consider:

$$x^3 - 2 = (x - \sqrt[3]{2})\left(x^2 + x\sqrt[3]{2} + \sqrt[3]{2}^2\right)$$
$$= (x - \sqrt[3]{2})\left(x - \left(\frac{1 + i\sqrt{3}}{2}\right)\sqrt[3]{2}\right)\left(x - \left(\frac{1 - i\sqrt{3}}{2}\right)\sqrt[3]{2}\right)$$

Well, that's ugly. Let's see if we can do better.

- Introduction
- Polynomials and Fundamental Theorem of Algebra
- Visualizing Complex Numbers
- Permuting Roots
- Fixed Fields and Groups

Complex Numbers

$$\mathbb{C} = \{z = a + bi : a, b \in \mathbb{R}\}$$

Complex Numbers

$$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$$

Complex Numbers

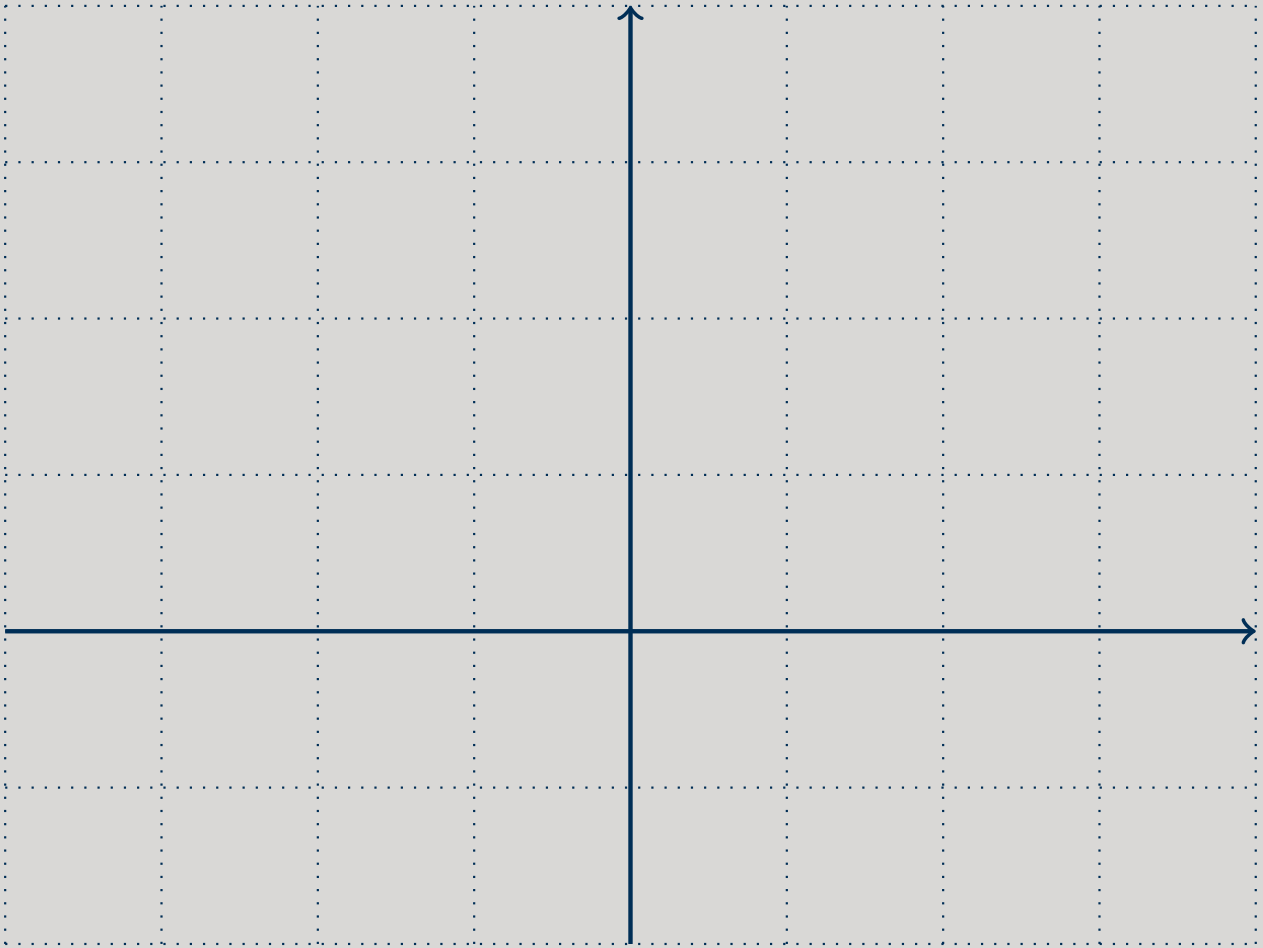
$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)

Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)

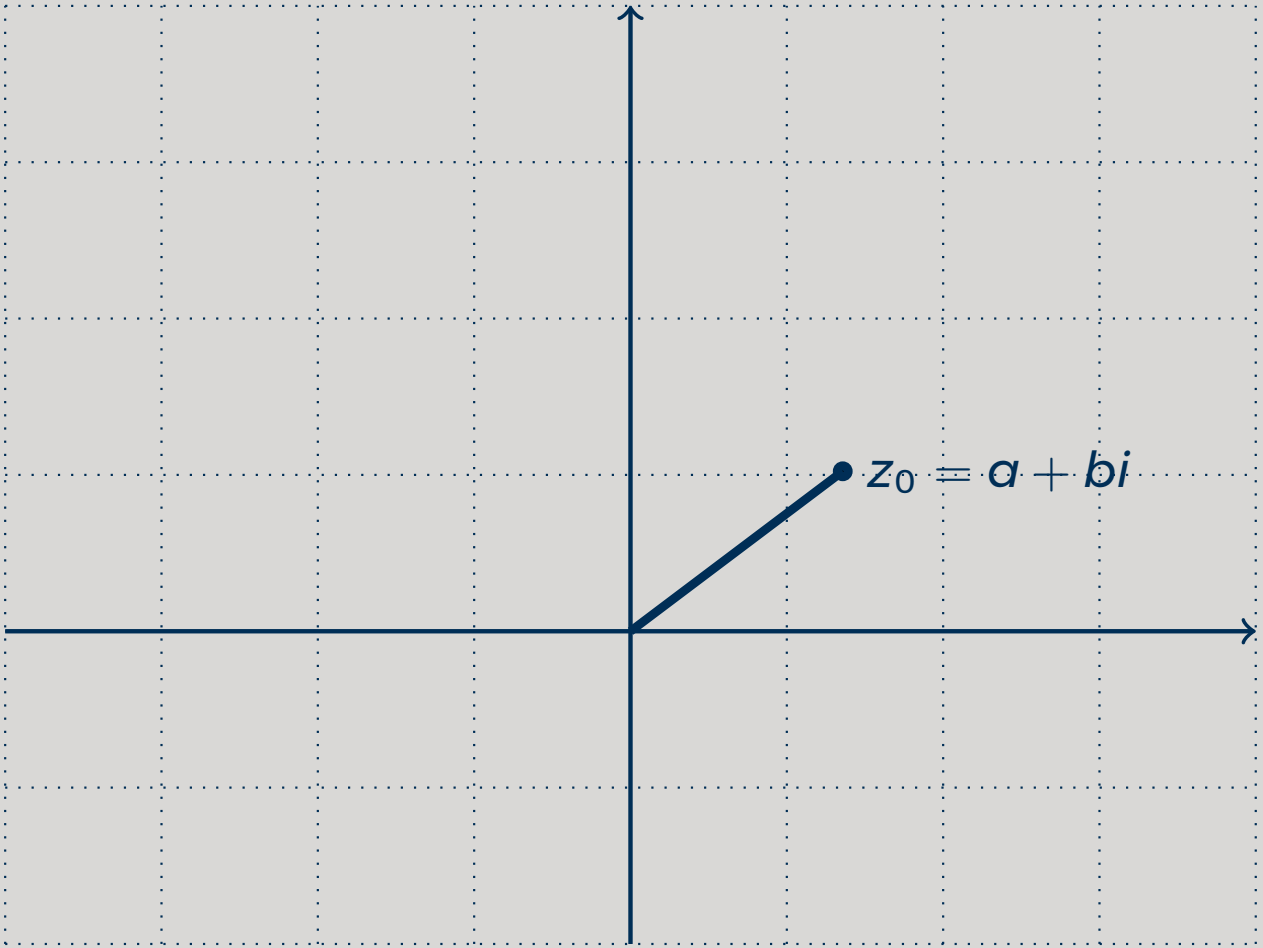
Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)



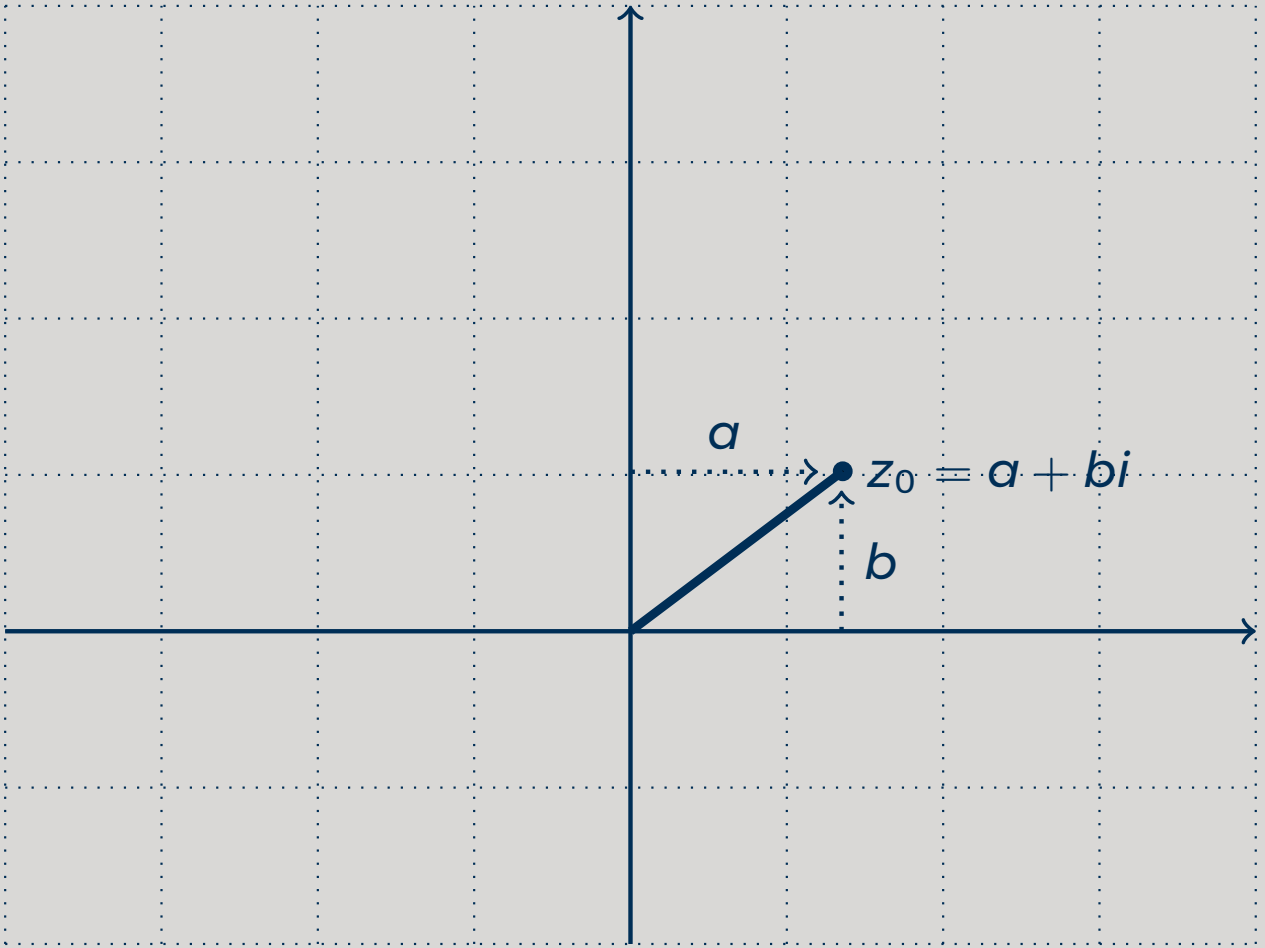
Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)



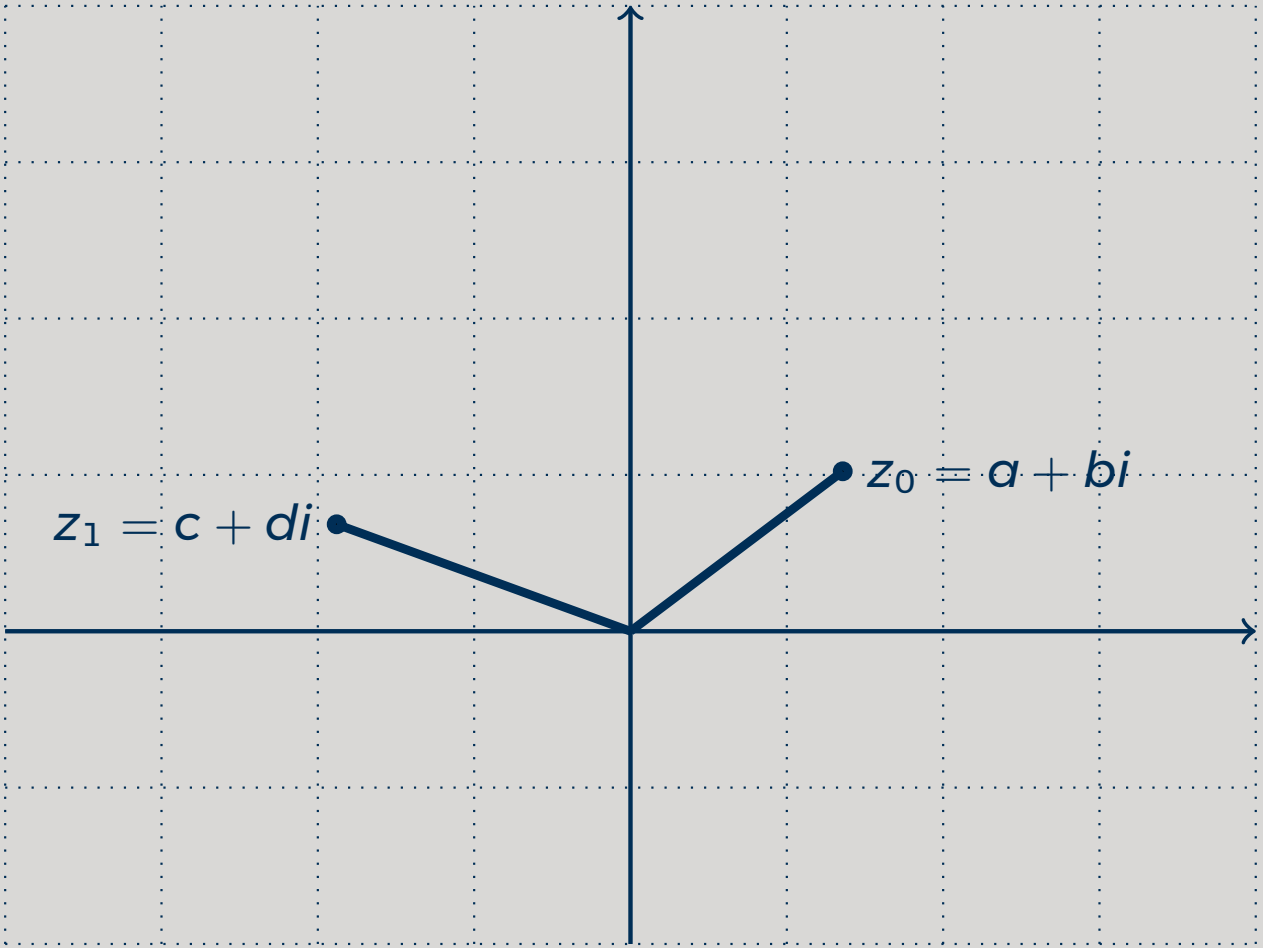
Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)



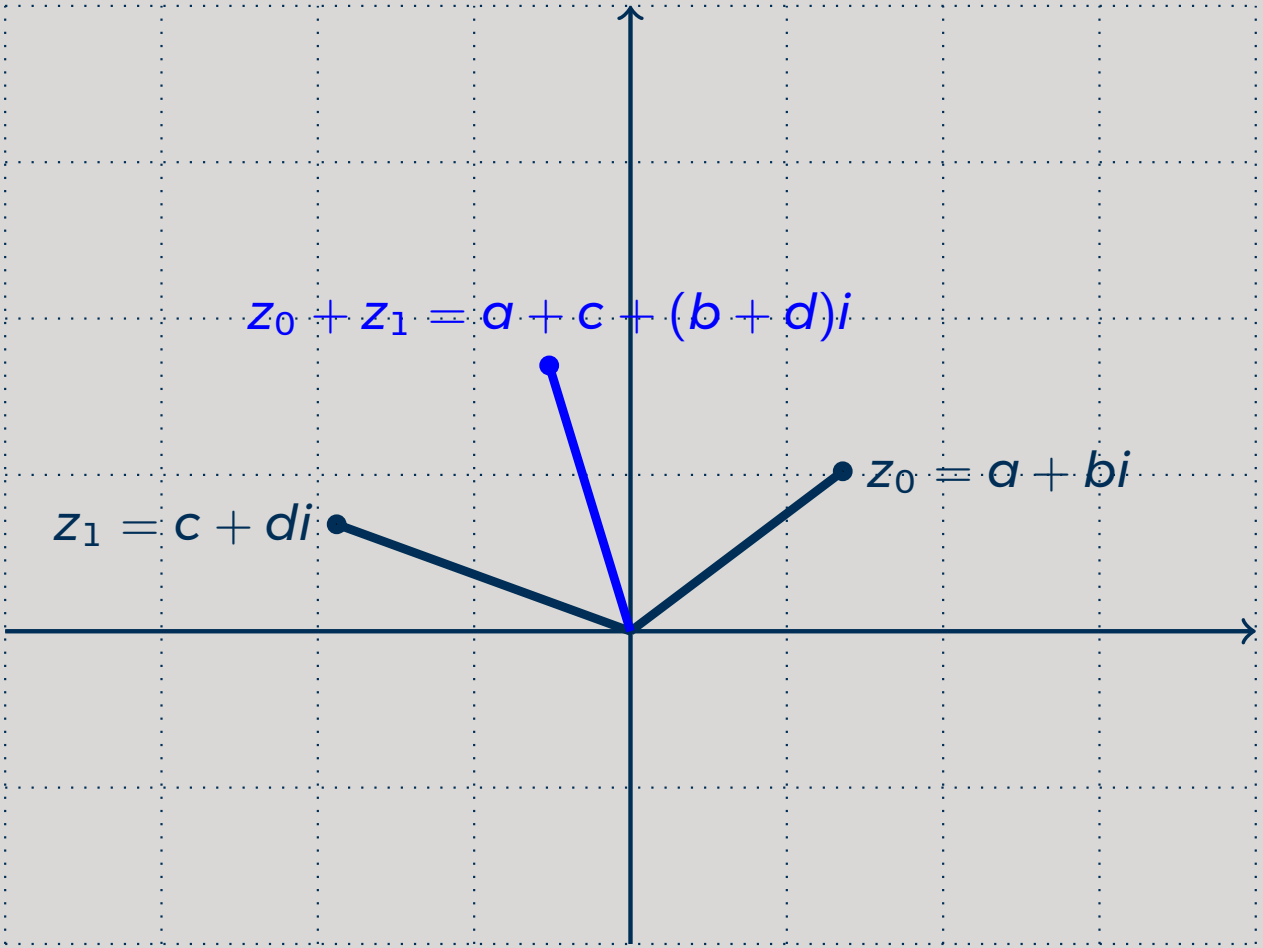
Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)



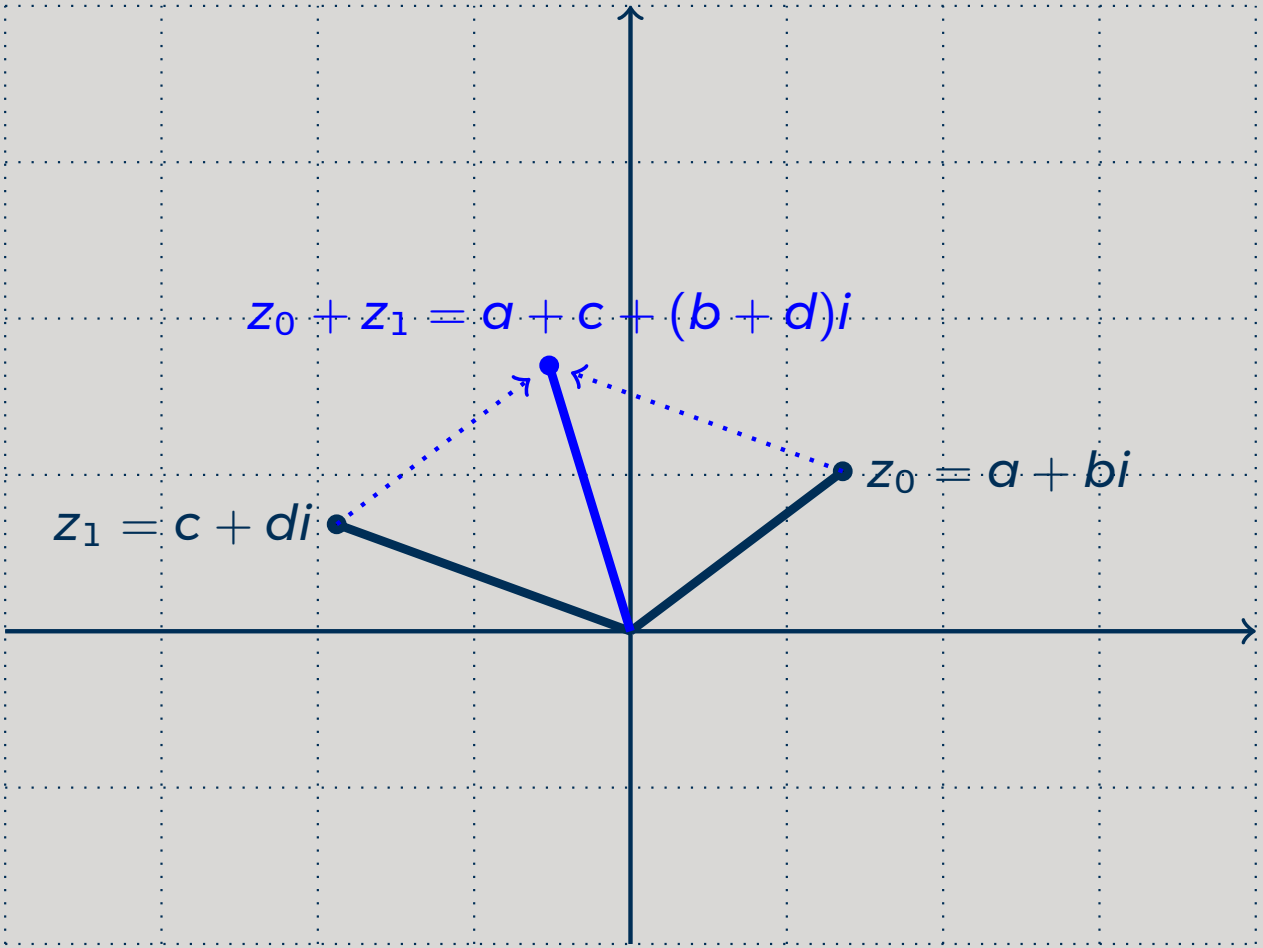
Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)



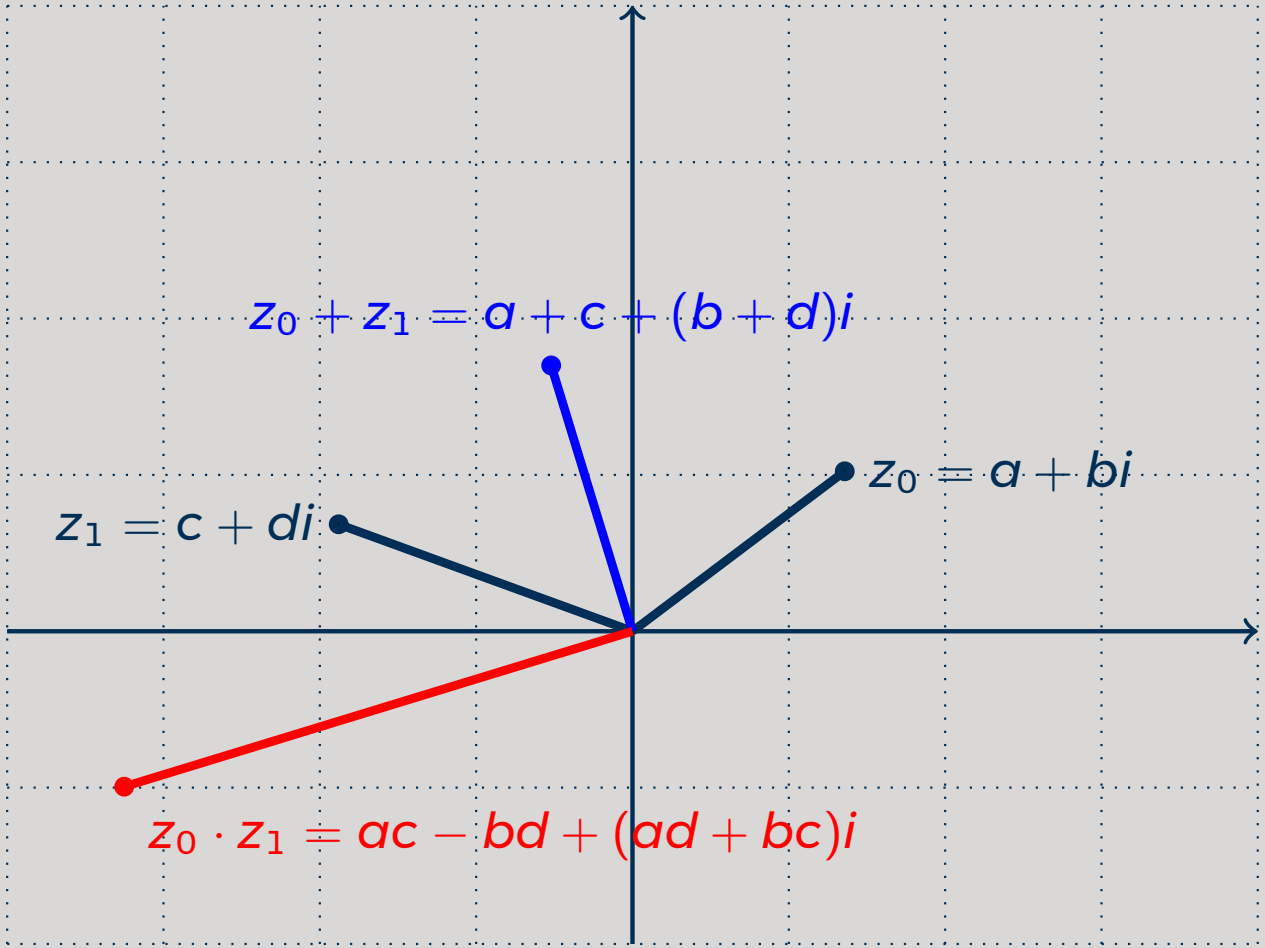
Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)



Complex Numbers

$\mathbb{R}[i] = \{z = a + bi : a, b \in \mathbb{R}\}$ (Called an *Extension*)



Roots of Unity:

- $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + x^{n-3} + \cdots + 1) = 0$

Roots of Unity:

- $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + x^{n-3} + \cdots + 1) = 0$
- De Moivre's Theorem: $(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$

Roots of Unity:

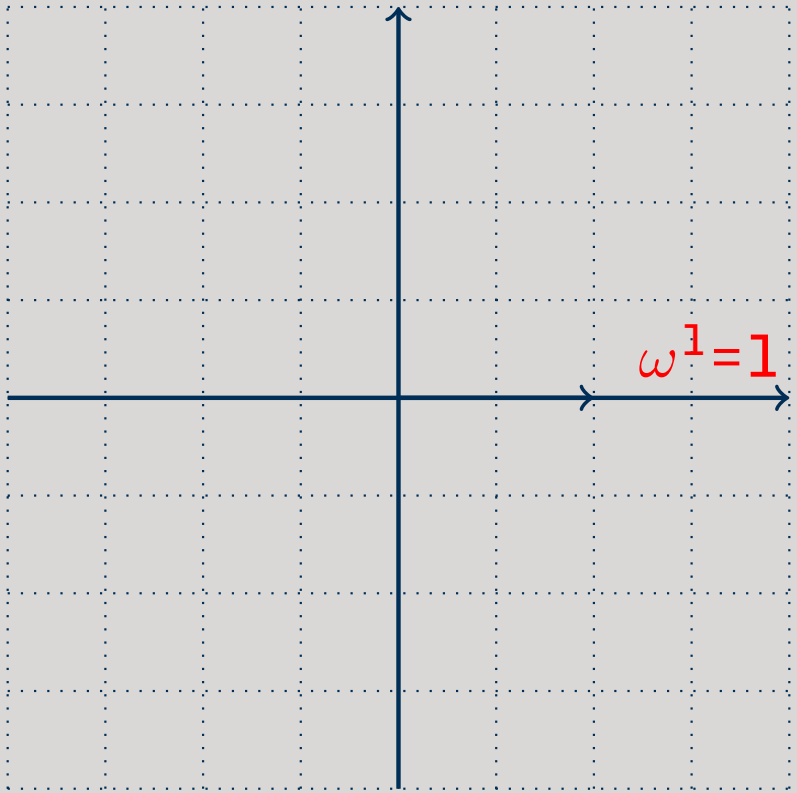
- $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + x^{n-3} + \cdots + 1) = 0$
- De Moivre's Theorem: $(\cos(\theta) + i\sin(\theta))^n = \cos(n\,\theta) + i\sin(n\,\theta)$
- $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$

Roots of Unity:

- $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + x^{n-3} + \cdots + 1) = 0$
- De Moivre's Theorem: $(\cos(\theta) + i\sin(\theta))^n = \cos(n\,\theta) + i\sin(n\,\theta)$
- $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$
- $\omega^n = (\cos(2\pi/n) + i\sin(2\pi/n))^n = \cos(2\pi) + i\sin(2\pi) = 1$

Roots of Unity:

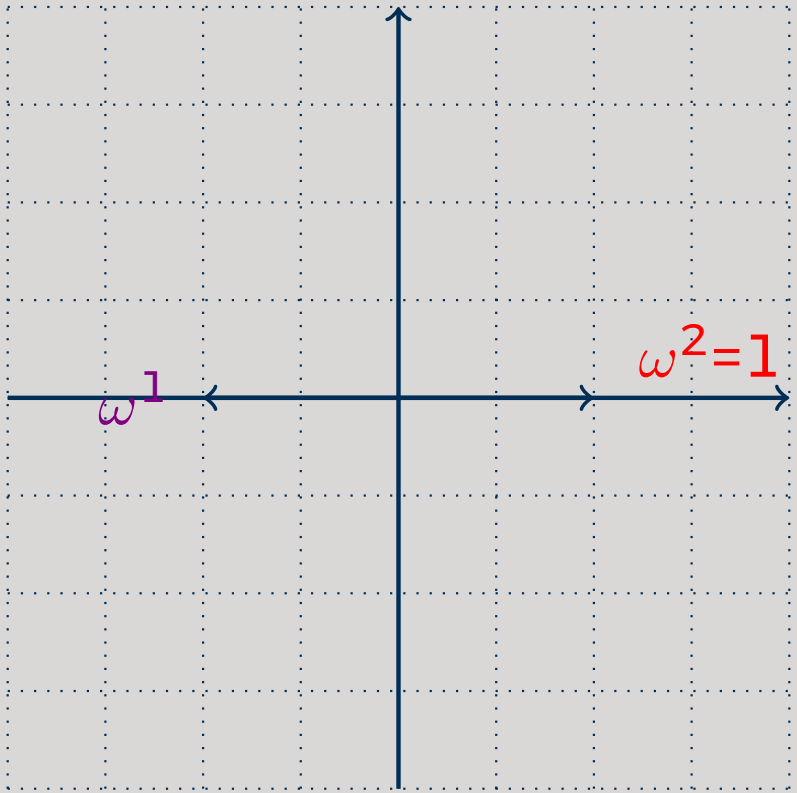
All the solutions to $x^1 - 1 = 0$



$$\omega = \cos(2\pi/1) + i\sin(2\pi/1)$$

Roots of Unity:

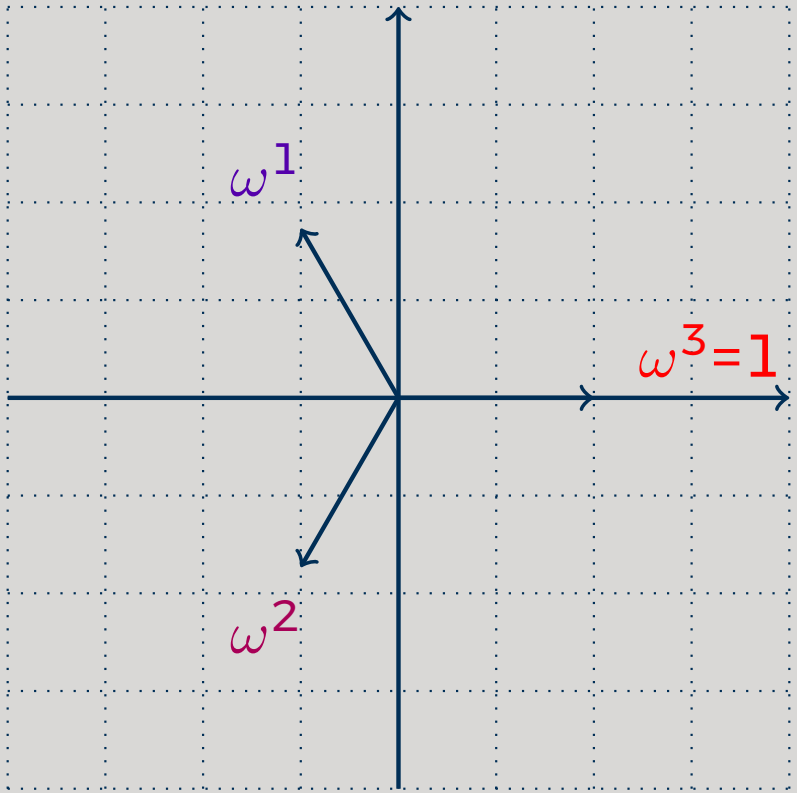
All the solutions to $x^2 - 1 = 0$



$$\omega = \cos(2\pi/2) + i\sin(2\pi/2)$$

Roots of Unity:

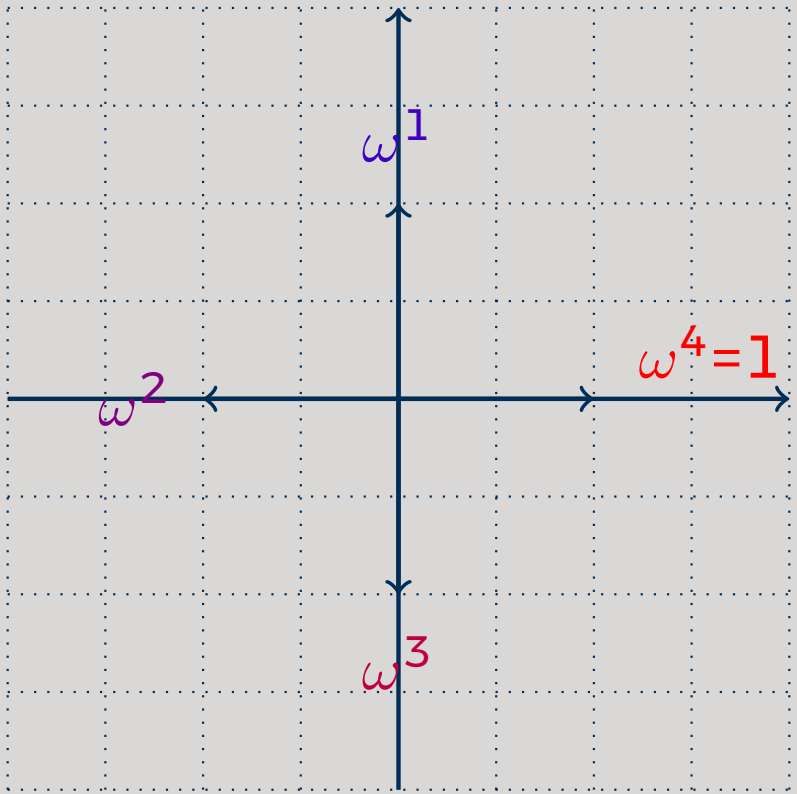
All the solutions to $x^3 - 1 = 0$



$$\omega = \cos(2\pi/3) + i\sin(2\pi/3)$$

Roots of Unity:

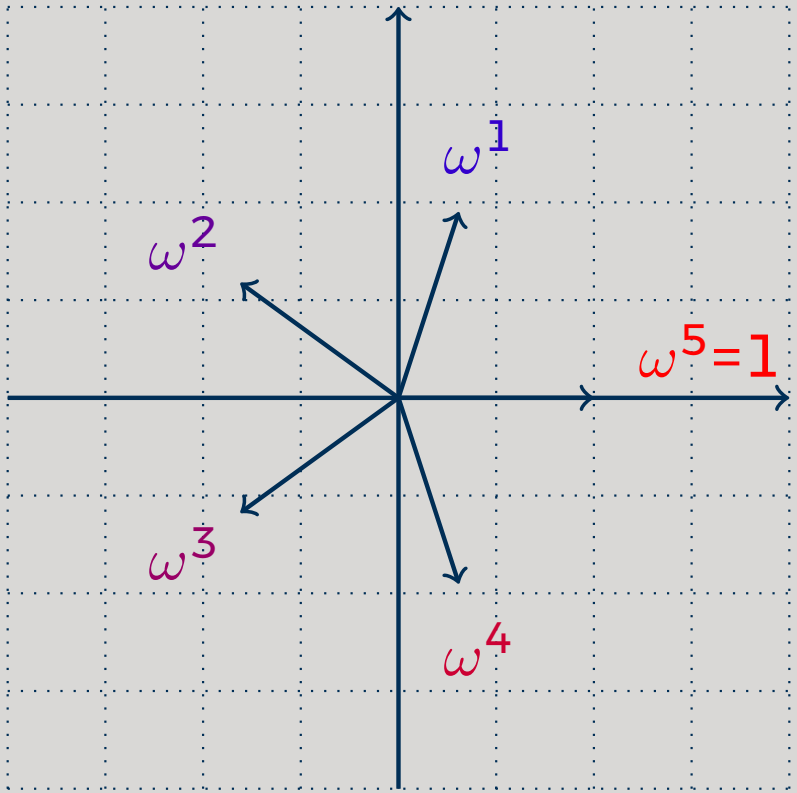
All the solutions to $x^4 - 1 = 0$



$$\omega = \cos(2\pi/4) + i\sin(2\pi/4)$$

Roots of Unity:

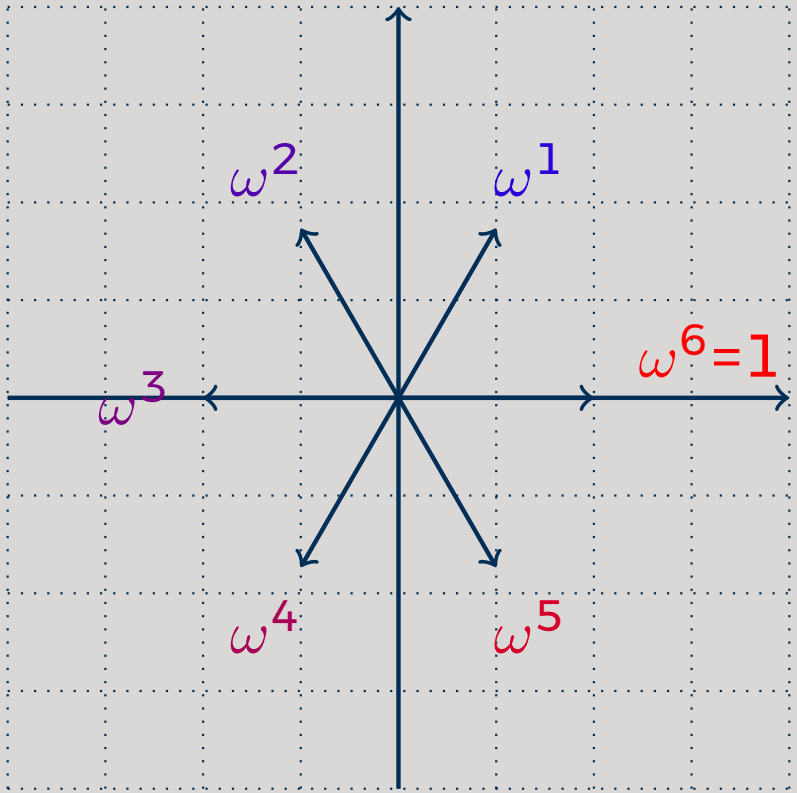
All the solutions to $x^5 - 1 = 0$



$$\omega = \cos(2\pi/5) + i\sin(2\pi/5)$$

Roots of Unity:

All the solutions to $x^6 - 1 = 0$



$$\omega = \cos(2\pi/6) + i\sin(2\pi/6)$$

Other Roots

- $x^n - k = 0$

Other Roots

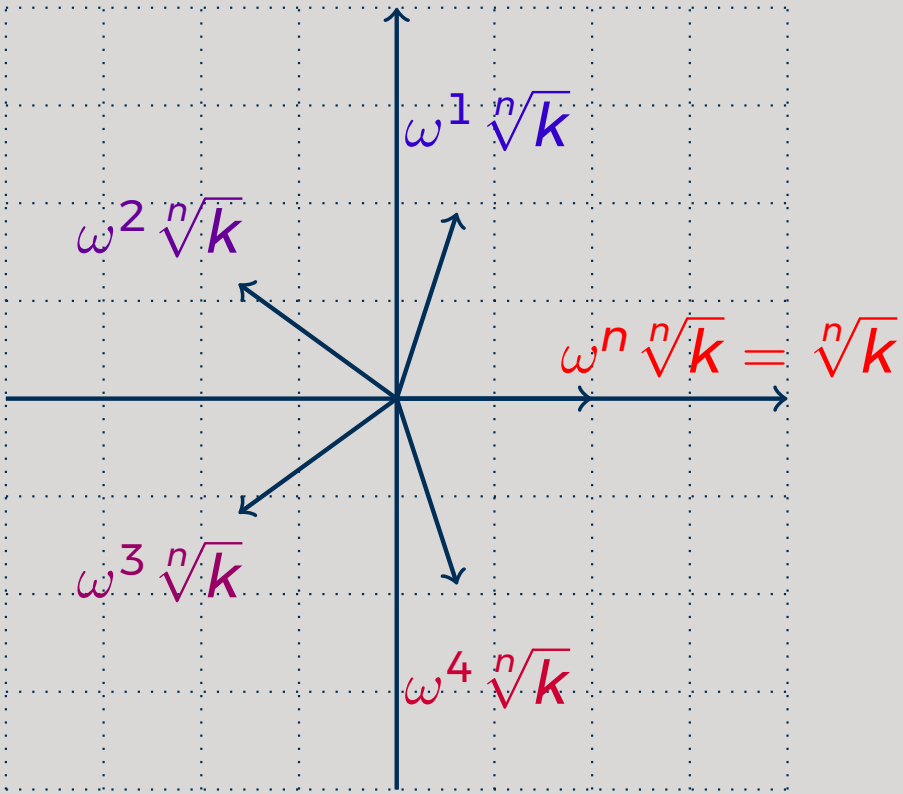
- $x^n - k = 0$
- $z = \omega^i \sqrt[n]{k}$, with $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$

Other Roots

- $x^n - k = 0$
- $z = \omega^i \sqrt[n]{k}$, with $\omega = \cos(2\pi/n) + i \sin(2\pi/n)$
- $z^n = (\omega^i)^n (\sqrt[n]{k})^n = (\omega^n)^i k = k$

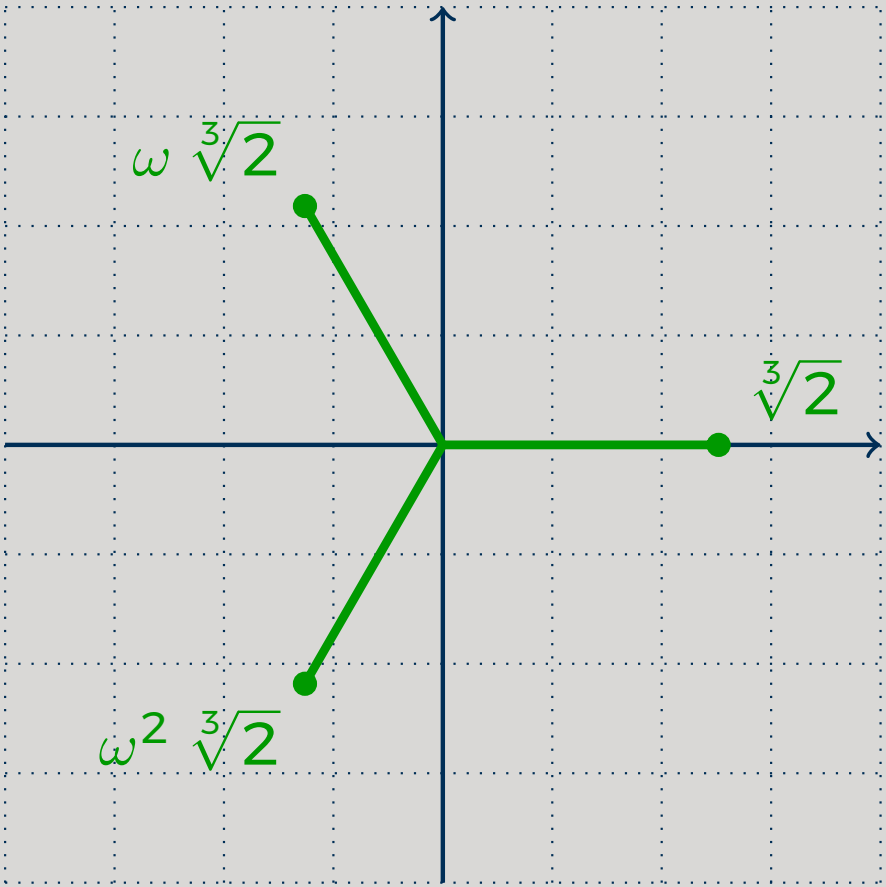
Other Roots

- $x^n - k = 0$
- $z = \omega^i \sqrt[n]{k}$, with $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$
- $z^n = (\omega^i)^n (\sqrt[n]{k})^n = (\omega^n)^i k = k$



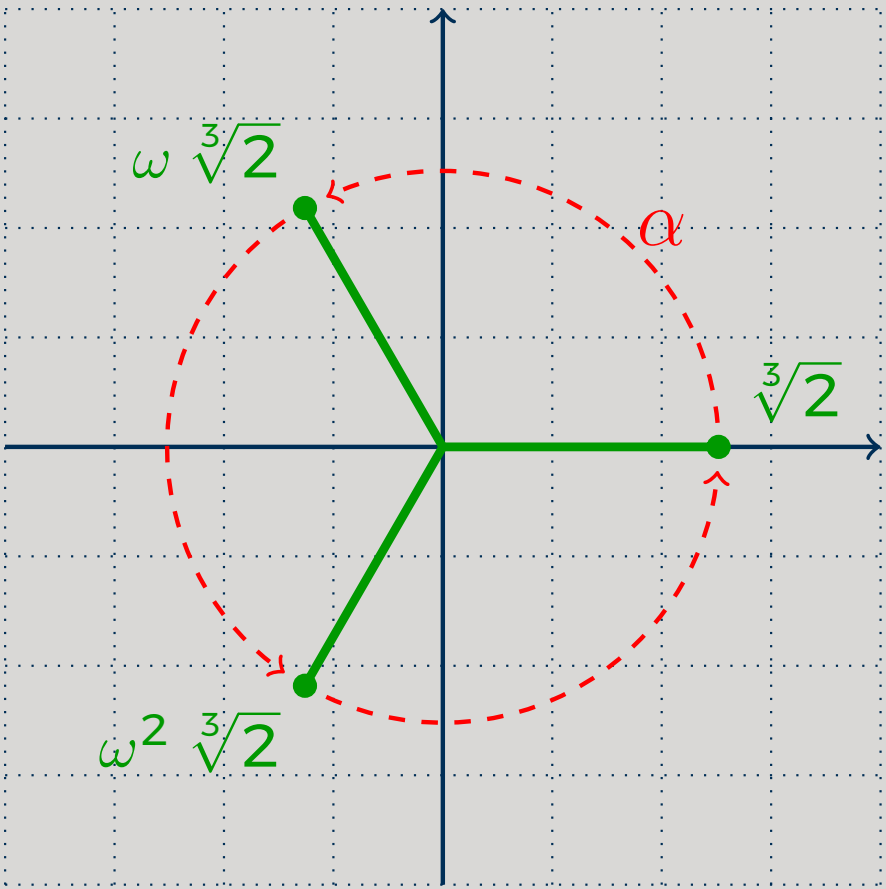
- Introduction
- Polynomials and Fundamental Theorem of Algebra
- Visualizing Complex Numbers
- Permuting Roots
- Fixed Fields and Groups

Permuting Roots Visually



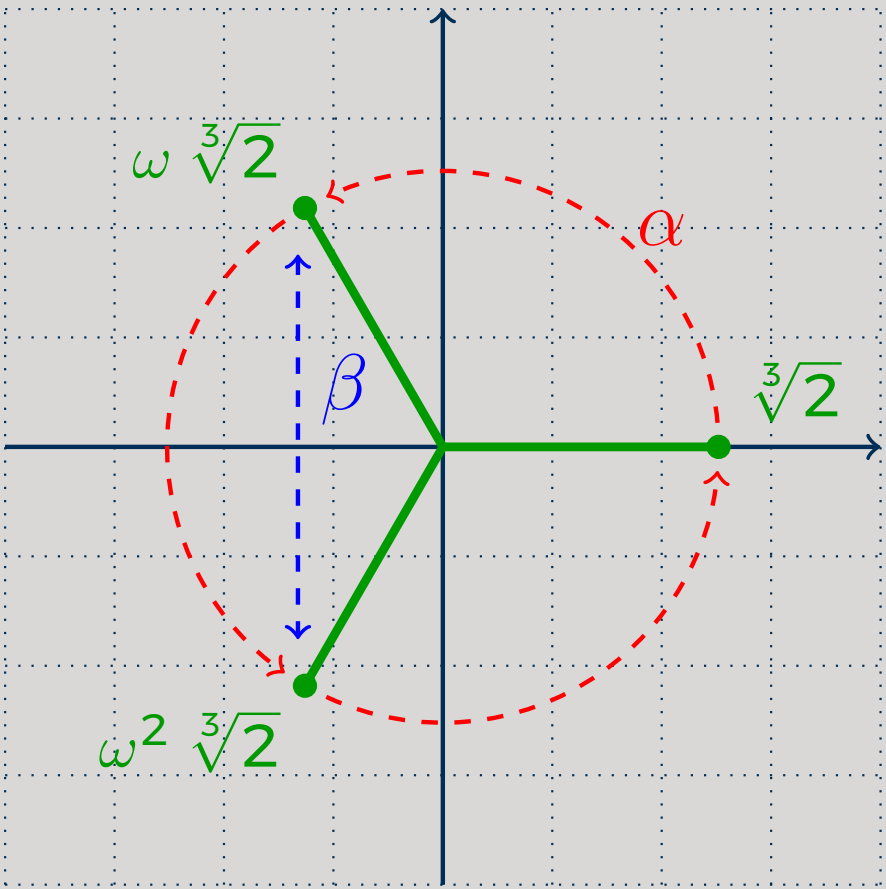
- Roots of $x^3 - 2$

Permuting Roots Visually



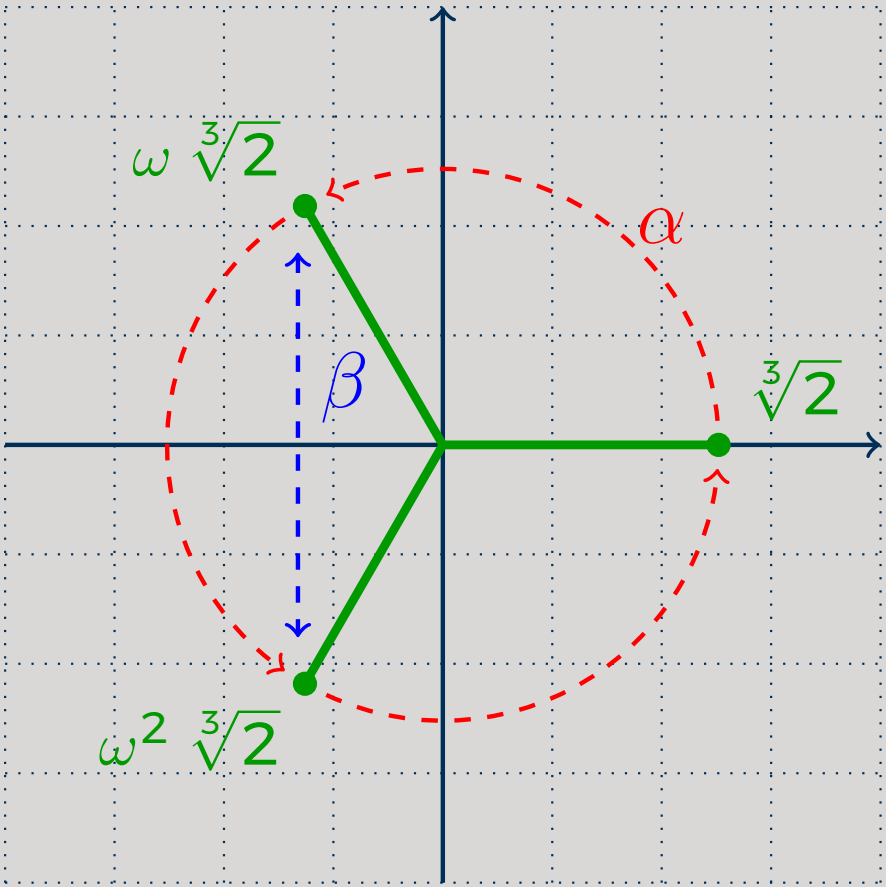
- Roots of $x^3 - 2$
- Cycling the Roots

Permuting Roots Visually



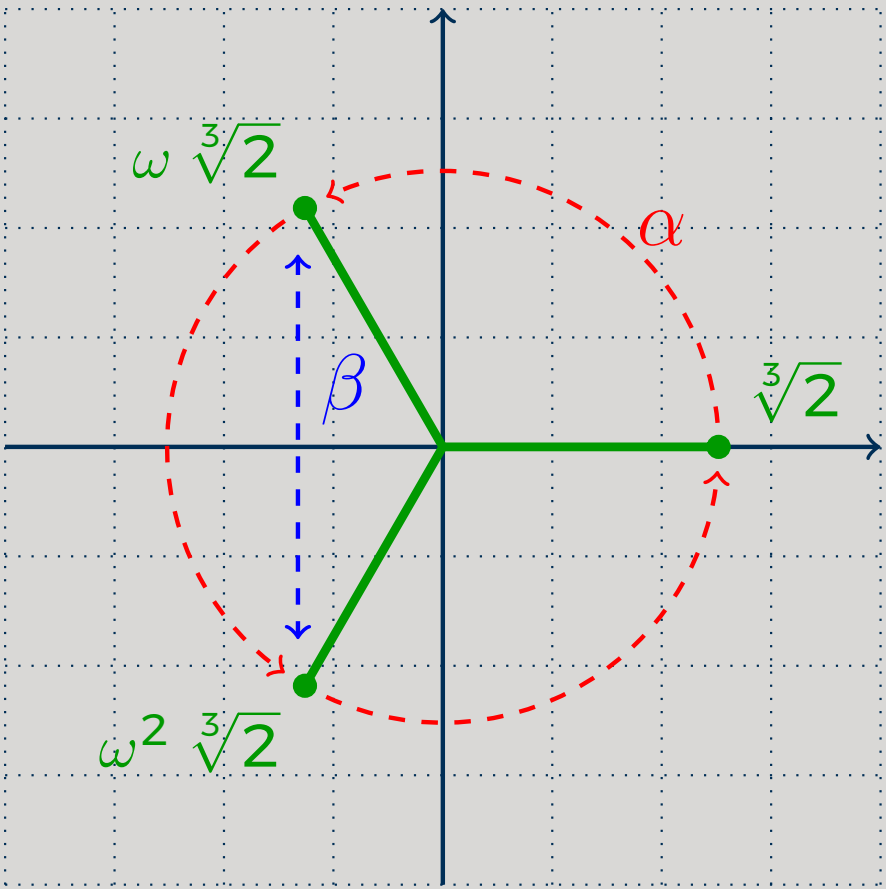
- Roots of $x^3 - 2$
- Cycling the Roots
- Swapping Two Roots

Permuting Roots Visually



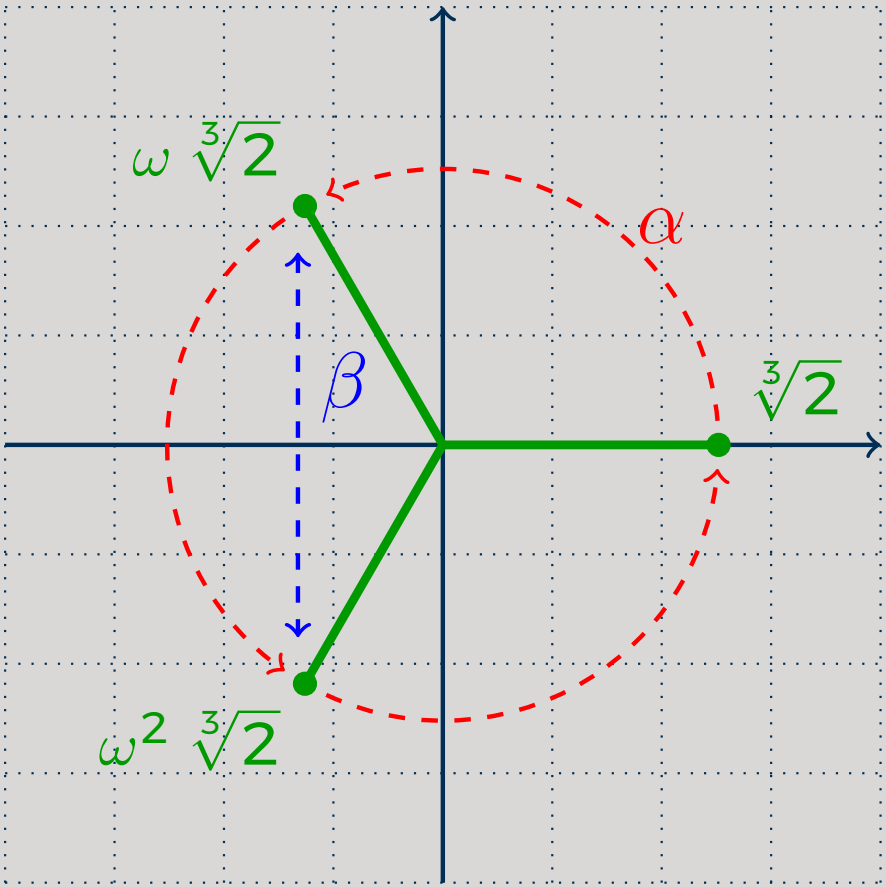
- Roots of $x^3 - 2$
- Cycling the Roots
- Swapping Two Roots
- Swapping the Others?

Permuting Roots Visually



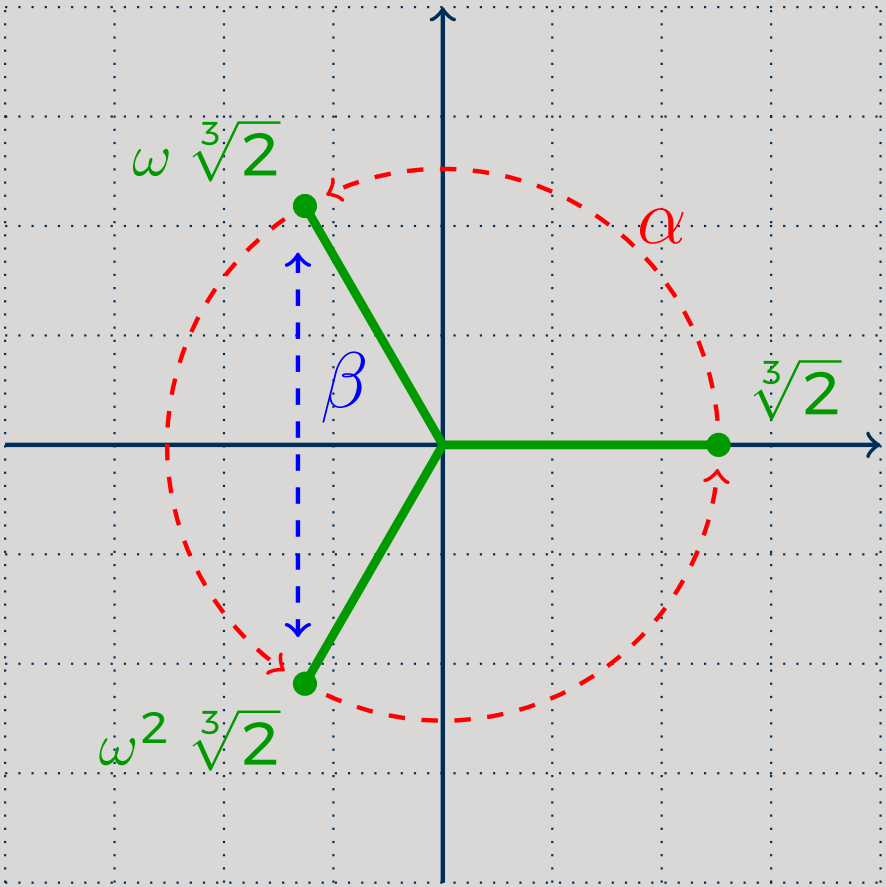
- Roots of $x^3 - 2$
- Cycling the Roots
- Swapping Two Roots
- Swapping the Others?
- Swap and Cycle vs. Cycle and Swap

Permuting Roots Visually



- Roots of $x^3 - 2$
- Cycling the Roots
- Swapping Two Roots
- Swapping the Others?
- Swap and Cycle vs. Cycle and Swap
- What does this remind us of?

Permuting Roots Visually



- Roots of $x^3 - 2$
- Cycling the Roots
- Swapping Two Roots
- Swapping the Others?
- Swap and Cycle vs. Cycle and Swap
- What does this remind us of?
- Only move the roots!

Permuting Roots with Automorphisms

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\zeta = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{2}^2 + g\omega^2 + h\omega^2\sqrt[3]{2} + k\omega^2\sqrt[3]{2}^2$$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\alpha\left(\sqrt[3]{2}\right)^3 =$$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\alpha\left(\sqrt[3]{2}\right)^3 = \alpha\left(\left(\sqrt[3]{2}\right)^3\right)$$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\begin{aligned}\alpha\left(\sqrt[3]{2}\right)^3 &= \alpha\left(\left(\sqrt[3]{2}\right)^3\right) \\ &= \alpha(2)\end{aligned}$$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\begin{aligned}\alpha\left(\sqrt[3]{2}\right)^3 &= \alpha\left(\left(\sqrt[3]{2}\right)^3\right)\\ &= \alpha(2)\\ &= 2,\end{aligned}$$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\begin{aligned}\alpha\left(\sqrt[3]{2}\right)^3 &= \alpha\left(\left(\sqrt[3]{2}\right)^3\right)\\ &= \alpha(2)\\ &= 2,\end{aligned}$$

$\alpha\left(\sqrt[3]{2}\right) = \sqrt[3]{2}, \omega\sqrt[3]{2}$, or $\omega^2\sqrt[3]{2}$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\begin{aligned}\alpha\left(\sqrt[3]{2}\right)^3 &= \alpha\left(\left(\sqrt[3]{2}\right)^3\right)\\ &= \alpha(2)\\ &= 2,\end{aligned}$$

$\alpha\left(\sqrt[3]{2}\right) = \sqrt[3]{2}, \omega\sqrt[3]{2}$, or $\omega^2\sqrt[3]{2}$

$$\sqrt[3]{2} \mapsto \sqrt[3]{2} \Longrightarrow \alpha = e$$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\begin{aligned}\alpha\left(\sqrt[3]{2}\right)^3 &= \alpha\left(\left(\sqrt[3]{2}\right)^3\right)\\ &= \alpha(2)\\ &= 2,\end{aligned}$$

$\alpha\left(\sqrt[3]{2}\right) = \sqrt[3]{2}, \omega\sqrt[3]{2}$, or $\omega^2\sqrt[3]{2}$

$\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ is the inverse of $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\begin{aligned}\alpha\left(\sqrt[3]{2}\right)^3 &= \alpha\left(\left(\sqrt[3]{2}\right)^3\right)\\ &= \alpha(2)\\ &= 2,\end{aligned}$$

$\alpha\left(\sqrt[3]{2}\right) = \sqrt[3]{2}, \omega\sqrt[3]{2}$, or $\omega^2\sqrt[3]{2}$

$$\alpha\left(\sqrt[3]{2}\right) = \omega\sqrt[3]{2}$$

Permuting Roots with Automorphisms

1^{st} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}[\omega]$

$$\begin{aligned}\alpha\left(\sqrt[3]{2}\right)^3 &= \alpha\left(\left(\sqrt[3]{2}\right)^3\right)\\ &= \alpha(2)\\ &= 2,\end{aligned}$$

$\alpha\left(\sqrt[3]{2}\right) = \sqrt[3]{2}, \omega\sqrt[3]{2}$, or $\omega^2\sqrt[3]{2}$

$$\alpha\left(\sqrt[3]{2}\right) = \omega\sqrt[3]{2}$$

Note $\alpha^3 = e$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\beta(\omega)^3 =$$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\beta(\omega)^3 = \beta\left(\omega^3\right)$$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\begin{aligned}\beta(\omega)^3 &= \beta\left(\omega^3\right)\\ &= \beta(1)\end{aligned}$$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\begin{aligned}\beta(\omega)^3 &= \beta\left(\omega^3\right)\\ &= \beta(1)\\ &= 1,\end{aligned}$$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\begin{aligned}\beta(\omega)^3 &= \beta\left(\omega^3\right)\\ &= \beta(1)\\ &= 1,\end{aligned}$$

$\beta(\omega) = 1, \omega$, or ω^2

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\begin{aligned}\beta(\omega)^3 &= \beta\left(\omega^3\right)\\ &= \beta(1)\\ &= 1,\end{aligned}$$

$\beta(\omega) = 1, \omega$, or ω^2

$\omega \mapsto 1 \Longrightarrow \beta$ is not 1-1 and not an automorphism

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\begin{aligned}\beta(\omega)^3 &= \beta\left(\omega^3\right)\\ &= \beta(1)\\ &= 1,\end{aligned}$$

$\beta(\omega) = 1, \omega$, or ω^2

$$\omega \mapsto \omega \Longrightarrow \beta = e$$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\begin{aligned}\beta(\omega)^3 &= \beta\left(\omega^3\right)\\ &= \beta(1)\\ &= 1,\end{aligned}$$

$\beta(\omega) = 1, \omega$, or ω^2

$$\beta(\omega) = \omega^2$$

Permuting Roots with Automorphisms

2^{nd} - Find an automorphism of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$ which "fixes" $\mathbb{Q}\left[\sqrt[3]{2}\right]$

$$\begin{aligned}\beta(\omega)^3 &= \beta\left(\omega^3\right)\\ &= \beta(1)\\ &= 1,\end{aligned}$$

$\beta(\omega) = 1, \omega$, or ω^2

$$\beta(\omega) = \omega^2$$

Note $\beta^2 = e$

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$
- β fixes $\mathbb{Q}\left[\sqrt[3]{2}\right]$

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$
- β fixes $\mathbb{Q}\left[\sqrt[3]{2}\right]$
- What about $\alpha \circ \beta$?

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$
- β fixes $\mathbb{Q}\left[\sqrt[3]{2}\right]$
- What about $\alpha \circ \beta$?

$$\alpha(\beta(\omega)) = \omega^2$$

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$
- β fixes $\mathbb{Q}\left[\sqrt[3]{2}\right]$
- What about $\alpha \circ \beta$?

$$\alpha(\beta(\omega)) = \omega^2$$

$$\alpha(\beta(\sqrt[3]{2})) = \omega\sqrt[3]{2}$$

Permuting Roots with Automorphisms

But, where does a general element, ζ, go?

Permuting Roots with Automorphisms

But, where does a general element, ζ, go?

$$\alpha \circ \beta(\zeta) =$$

Permuting Roots with Automorphisms

But, where does a general element, ζ, go?

$$\alpha \circ \beta(\zeta) = \alpha\left(\beta\left(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{2}^2 + g\omega^2 + h\omega^2\sqrt[3]{2} + k\omega^2\sqrt[3]{2}^2\right)\right)$$

Permuting Roots with Automorphisms

But, where does a general element, ζ, go?

$$\begin{aligned}\alpha \circ \beta(\zeta) = \alpha\Big(\beta\Big(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\omega\sqrt[3]{2} \\ + f\omega\sqrt[3]{2}^2 + g\omega^2 + h\omega^2\sqrt[3]{2} + k\omega^2\sqrt[3]{2}^2\Big)\Big) \\ = a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{2}^2 + d\omega^2 + e\sqrt[3]{2} \\ + f\omega\sqrt[3]{2}^2 + g\omega + h\omega^2\sqrt[3]{2} + k\sqrt[3]{2}^2\end{aligned}$$

Permuting Roots with Automorphisms

But, where does a general element, ζ, go?

$$\begin{aligned}\alpha \circ \beta(\zeta) = \alpha\Big(\beta\Big(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\omega\sqrt[3]{2} \\ + f\omega\sqrt[3]{2}^2 + g\omega^2 + h\omega^2\sqrt[3]{2} + k\omega^2\sqrt[3]{2}^2\Big)\Big) \\ = a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{2}^2 + d\omega^2 + e\sqrt[3]{2} \\ + f\omega\sqrt[3]{2}^2 + g\omega + h\omega^2\sqrt[3]{2} + k\sqrt[3]{2}^2\end{aligned}$$

Supposing ζ is fixed ...

Permuting Roots with Automorphisms

But, where does a general element, ζ, go?

$$\begin{aligned}\alpha \circ \beta(\zeta) = \alpha\Big(\beta\Big(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\omega\sqrt[3]{2} \\ + f\omega\sqrt[3]{2}^2 + g\omega^2 + h\omega^2\sqrt[3]{2} + k\omega^2\sqrt[3]{2}^2\Big)\Big) \\ = a + b\omega\sqrt[3]{2} + c\omega^2\sqrt[3]{2}^2 + d\omega^2 + e\sqrt[3]{2} \\ + f\omega\sqrt[3]{2}^2 + g\omega + h\omega^2\sqrt[3]{2} + k\sqrt[3]{2}^2\end{aligned}$$

Supposing ζ is fixed ...

$$a = a \qquad b = e \qquad c = k$$
$$d = g \qquad f = f \qquad h = h$$

Permuting Roots with Automorphisms

Supposing ζ is fixed ...

$$a = a \qquad b = e \qquad c = k$$
$$d = g \qquad f = f \qquad h = h$$

So ...

$$\zeta = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + e\omega\sqrt[3]{2} + f\omega\sqrt[3]{2}^2 + g\omega^2 + h\omega^2\sqrt[3]{2} + k\omega^2\sqrt[3]{2}^2$$

Permuting Roots with Automorphisms

Supposing ζ is fixed ...

$$a = a \qquad b = e \qquad c = k$$
$$d = g \qquad f = f \qquad h = h$$

So ...

$$\zeta = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + d\omega + b\omega\sqrt[3]{2} + f\omega\sqrt[3]{2}^2 + d\omega^2 + h\omega^2\sqrt[3]{2} + c\omega^2\sqrt[3]{2}^2$$

Permuting Roots with Automorphisms

So ...

$$\zeta = a + b\left(\sqrt[3]{2} + \omega\sqrt[3]{2}\right) + c\left(\sqrt[3]{2}^2 + \omega^2\sqrt[3]{2}^2\right)$$
$$+ d\left(\omega + \omega^2\right) + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2}$$

Permuting Roots with Automorphisms

So ...

$$\zeta = (a - d) + b\sqrt[3]{2}\,(1 + \omega) + c\sqrt[3]{2}^2\left(1 + \omega^2\right) + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2}$$

Permuting Roots with Automorphisms

So ...

$$\begin{aligned}\zeta &= (a-d) + b\sqrt[3]{2}\,(1+\omega) + c\sqrt[3]{2}^2\left(1+\omega^2\right) + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2} \\ &= (a-d) - b\omega^2\sqrt[3]{2} - c\omega\sqrt[3]{2}^2 + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2}\end{aligned}$$

Permuting Roots with Automorphisms

So ...

$$\zeta = (a-d) + b\sqrt[3]{2}\,(1+\omega) + c\sqrt[3]{2}^2\left(1+\omega^2\right) + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2}$$

$$= (a-d) - b\omega^2\sqrt[3]{2} - c\omega\sqrt[3]{2}^2 + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2}$$

Why does $1+\omega = -\omega^2$ and $1+\omega^2 = -\omega$ and $\omega+\omega^2 = -1$?

Permuting Roots with Automorphisms

So ...

$$\begin{aligned}\zeta &= (a-d) + b\sqrt[3]{2}\,(1+\omega) + c\sqrt[3]{2}^2\left(1+\omega^2\right) + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2} \\ &= (a-d) - b\omega^2\sqrt[3]{2} - c\omega\sqrt[3]{2}^2 + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2} \\ &= (a-d) + (h-b)\omega^2\sqrt[3]{2} + (f-c)\omega\sqrt[3]{2}^2\end{aligned}$$

Permuting Roots with Automorphisms

So ...

$$\begin{aligned}\zeta &= (a-d) + b\sqrt[3]{2}\,(1+\omega) + c\sqrt[3]{2}^2\left(1+\omega^2\right) + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2} \\ &= (a-d) - b\omega^2\sqrt[3]{2} - c\omega\sqrt[3]{2}^2 + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2} \\ &= (a-d) + (h-b)\omega^2\sqrt[3]{2} + (f-c)\omega\sqrt[3]{2}^2 \\ &= (a-d) + (h-b)\omega^2\sqrt[3]{2} + (f-c)\left(\omega^2\sqrt[3]{2}\right)^2\end{aligned}$$

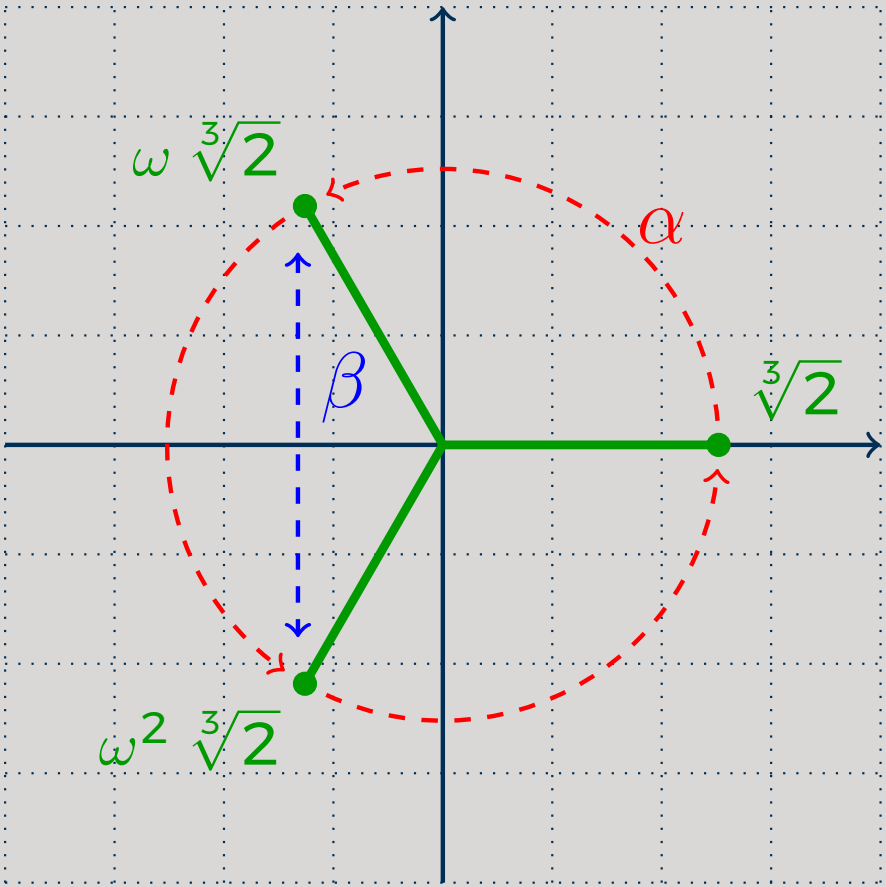
Permuting Roots with Automorphisms

So ...

$$\begin{aligned}\zeta &= (a-d) + b\sqrt[3]{2}\,(1+\omega) + c\sqrt[3]{2}^2\left(1+\omega^2\right) + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2} \\ &= (a-d) - b\omega^2\sqrt[3]{2} - c\omega\sqrt[3]{2}^2 + f\omega\sqrt[3]{2}^2 + h\omega^2\sqrt[3]{2} \\ &= (a-d) + (h-b)\omega^2\sqrt[3]{2} + (f-c)\omega\sqrt[3]{2}^2 \\ &= (a-d) + (h-b)\omega^2\sqrt[3]{2} + (f-c)\left(\omega^2\sqrt[3]{2}\right)^2\end{aligned}$$

And thus $\zeta \in \mathbb{Q}\left[\omega^2\sqrt[3]{2}\right]$

Permuting Roots Visually



- Roots of $x^3 - 2$
- Cycling the Roots
- Swapping Two Roots
- Swapping the Others?
- Swap and Cycle vs. Cycle and Swap
- What does this remind us of?
- Only move the roots!

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$
- β fixes $\mathbb{Q}\left[\sqrt[3]{2}\right]$
- What about $\alpha \circ \beta$?

$$\alpha(\beta(\omega)) = \omega^2$$

$$\alpha(\beta(\sqrt[3]{2})) = \omega\sqrt[3]{2}$$

- What about $\beta \circ \alpha^2$?

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$
- β fixes $\mathbb{Q}\left[\sqrt[3]{2}\right]$
- What about $\alpha \circ \beta$?

$$\alpha(\beta(\omega)) = \omega^2$$

$$\alpha(\beta(\sqrt[3]{2})) = \omega\sqrt[3]{2}$$

- What about $\beta \circ \alpha^2$?
- What about $\alpha^2 \circ \beta$?

Permuting Roots with Automorphisms

3^{rd} - How do α and β effect elements of $\mathbb{Q}\left[\omega, \sqrt[3]{2}\right]$?

- α fixes $\mathbb{Q}[\omega]$
- β fixes $\mathbb{Q}\left[\sqrt[3]{2}\right]$
- What about $\alpha \circ \beta$?

$$\alpha(\beta(\omega)) = \omega^2$$

$$\alpha(\beta(\sqrt[3]{2})) = \omega\sqrt[3]{2}$$

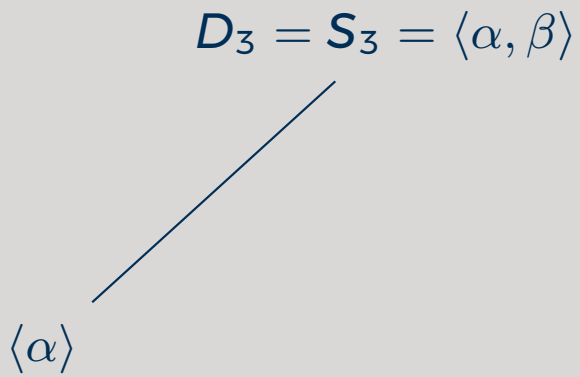
- What about $\beta \circ \alpha^2$?
- What about $\alpha^2 \circ \beta$?
- How many different possibilities are there?

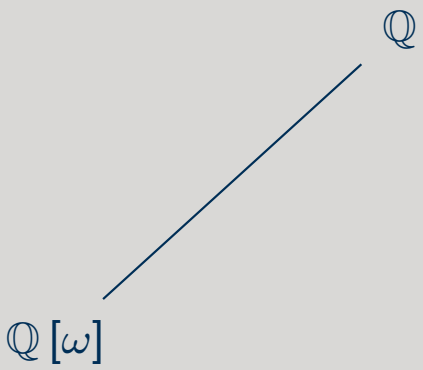
- Introduction
- Polynomials and Fundamental Theorem of Algebra
- Visualizing Complex Numbers
- Permuting Roots
- Fixed Fields and Groups

Fixed Fields and Groups

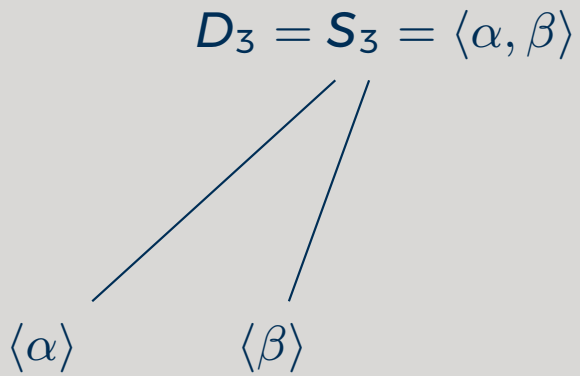
$D_3 = S_3 = \langle \alpha, \beta \rangle$ $\mathbb{Q}$

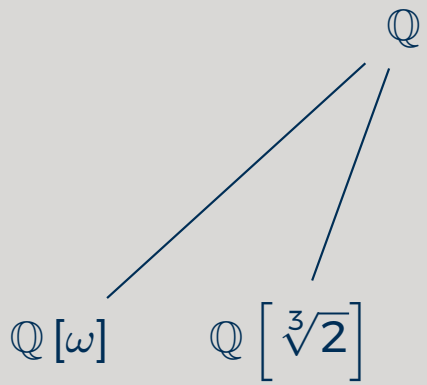
Fixed Fields and Groups



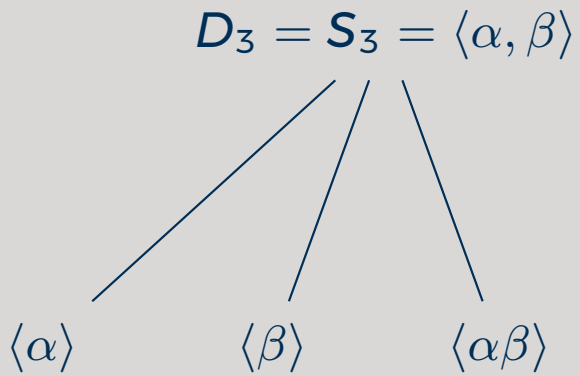


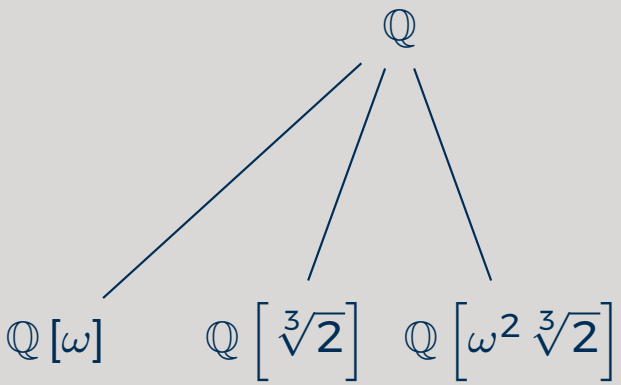
Fixed Fields and Groups



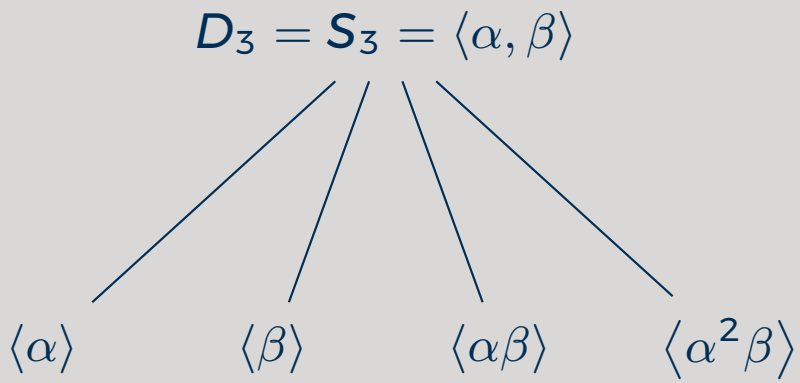


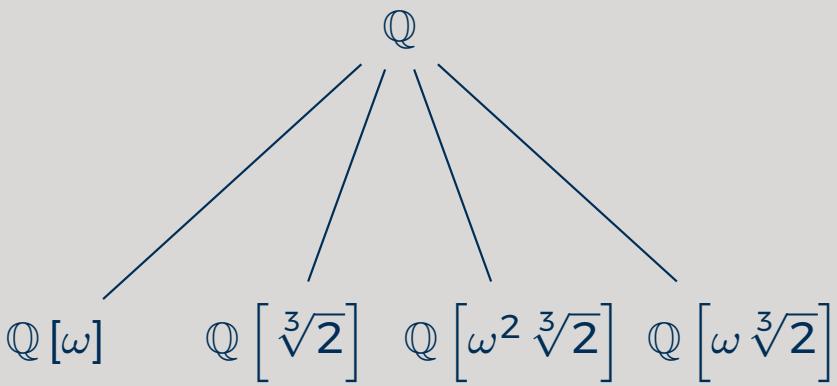
Fixed Fields and Groups



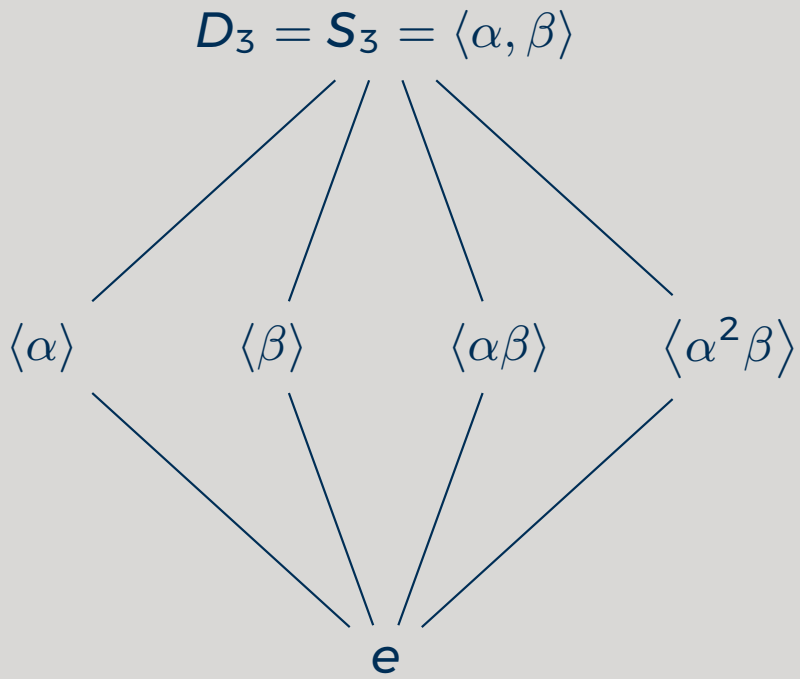


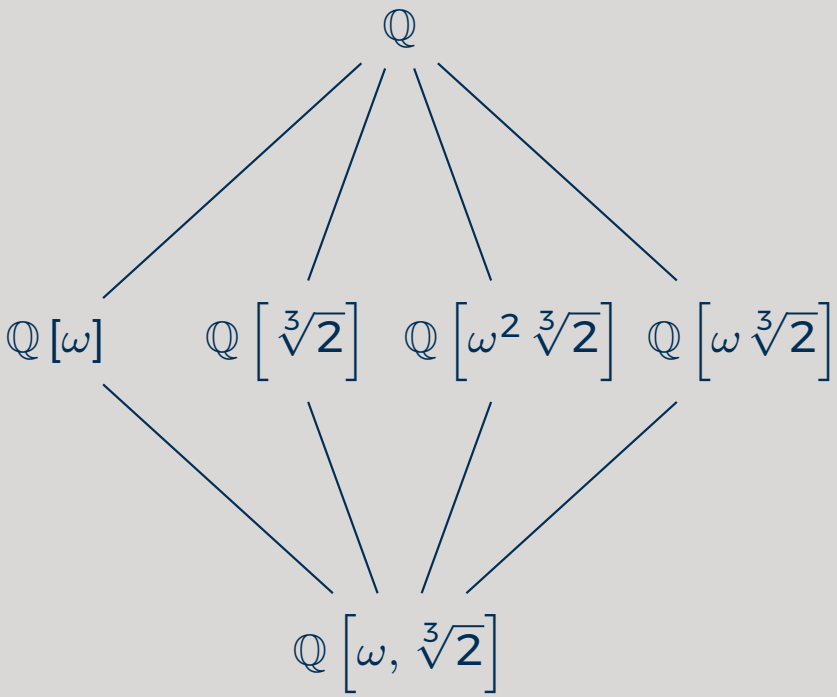
Fixed Fields and Groups



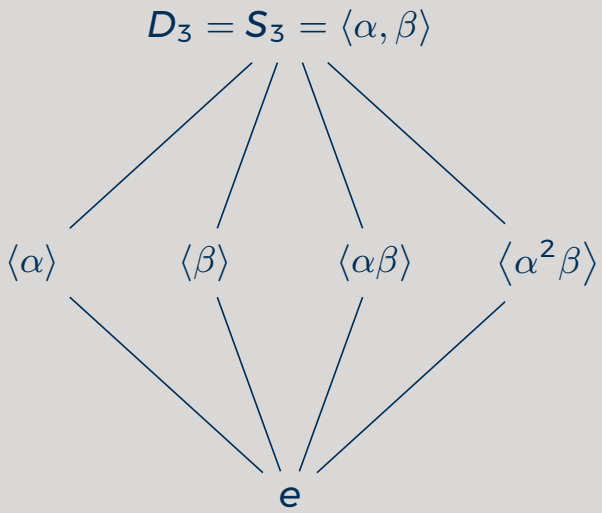


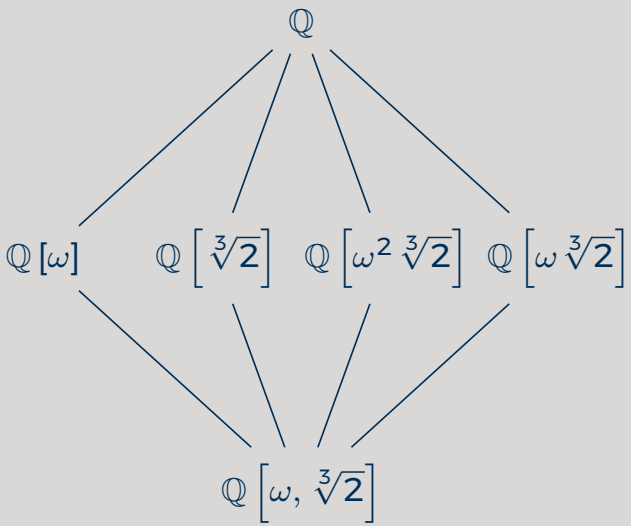
Fixed Fields and Groups





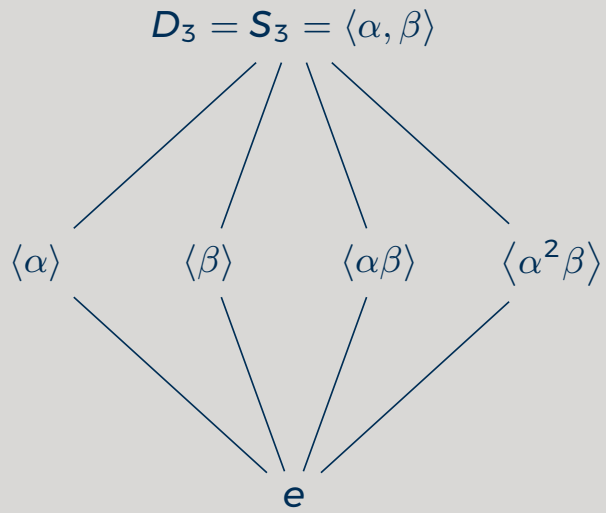
Fixed Fields and Groups

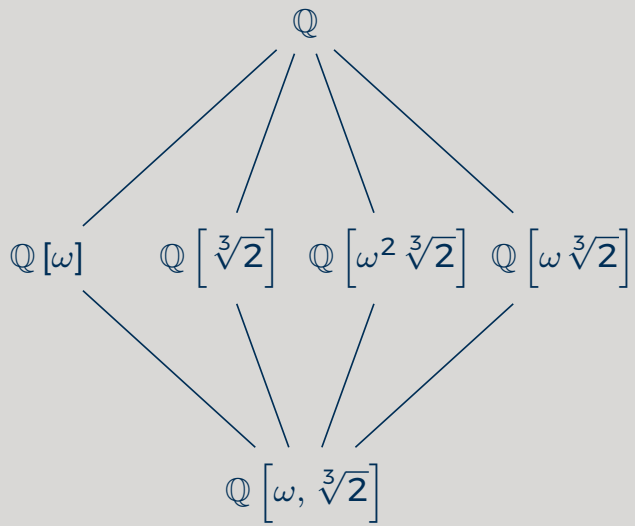




Notes:

Fixed Fields and Groups

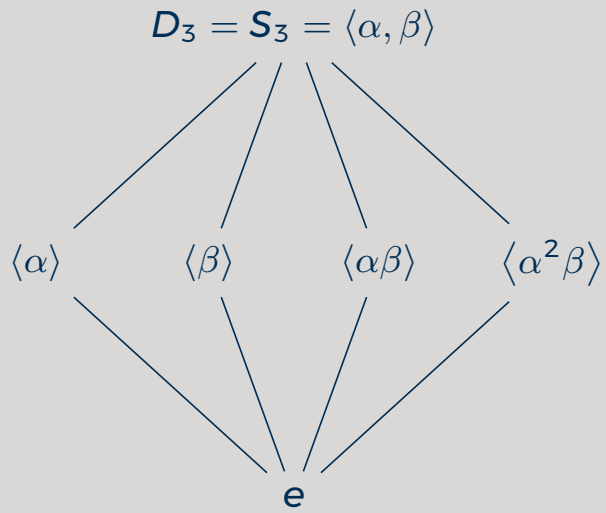


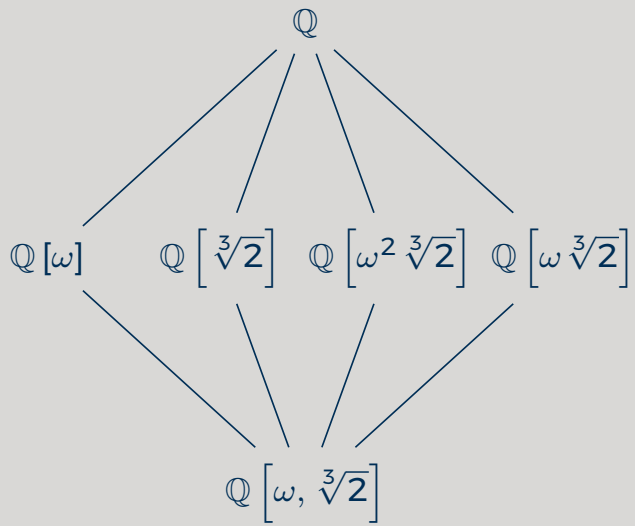


Notes:

- Groups get smaller the corresponding fields get larger.

Fixed Fields and Groups

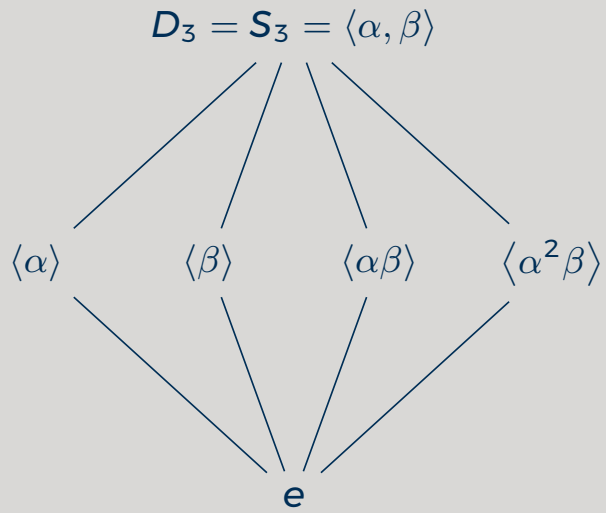


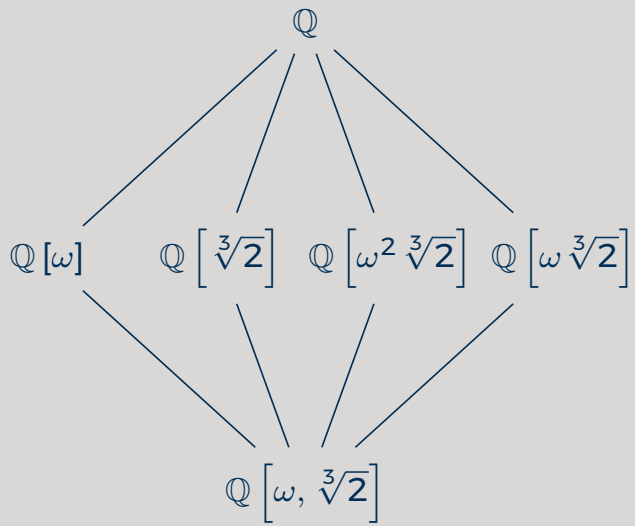


Notes:

- Groups get smaller the corresponding fields get larger.
- Subgroup indices match the degree of the *"minimal polynomial"* for the adjoined root.

Fixed Fields and Groups





Notes:

- Groups get smaller the corresponding fields get larger.
- Subgroup indices match the degree of the *"minimal polynomial"* for the adjoined root.
- The minimal polynomial only factors completely if the subgroup is normal.

Great Big Galois Example

Dr. Chuck Rocca
roccac@wcsu.edu

http://sites.wcsu.edu/roccac