Eine kleine Galoistheorie : une introduction en mots artistiques aux découvertes d'Évariste Galois, mathématicien mozartistique

Douglas Hofstadter

28 octobre 2007

←

Henri Poincaré, sur les analystes et leurs très, très longs calculs :

Croira-t-on... qu'ils ont toujours marché pas à pas, sans avoir la vision du but qu'ils voulaient atteindre ?

Il a bien fallu qu'ils devinassent le chemin qui y conduisait, et pour cela ils ont eu besoin d'un guide.

Ce guide, c'est d'abord l'analogie.

Le mystère et l'attraction des équations polynomiales

L'équation quadratique

$$x^2 + bx + c = 0$$

Al-Khwarizmi, $\sim$ 800

L'équation cubique

$$x^3 + bx^2 + cx + d = 0$$

del Ferro, Tartaglia, Cardan, Bombelli, $\sim$ 1500, 1600

L'équation quartique

$$x^4 + bx^3 + cx^2 + dx + e = 0$$

Cardan, Ferrari, $\sim$ 1545

L'équation quintique

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

Lagrange, Vandermonde, Ruffini, Abel, Galois, $\sim$ 1800

Les clés les plus simples suffiront-elles ?

$$\left.\begin{array}{lcl} x^2 - a = 0 & \longrightarrow & \sqrt{a} \\ x^3 - a = 0 & \longrightarrow & \sqrt[3]{a} \\ x^4 - a = 0 & \longrightarrow & \sqrt[4]{a} \\ x^5 - a = 0 & \longrightarrow & \sqrt[5]{a} \\ \vdots & \vdots & \vdots \end{array}\right\} \text{radicaux}$$

La force fourvoyante de l'analogie

L'équation *quadratique* se résout ainsi : $\dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$

(racine quadratique)

L'équation *cubique* se résout ainsi : $\sqrt[3]{r + \sqrt{\Delta}} + \sqrt[3]{r - \sqrt{\Delta}}$

(racines cubique et quadratique)

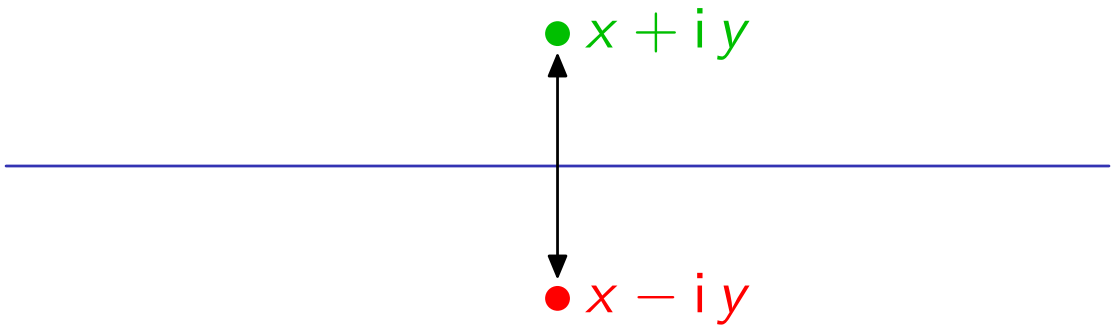
L'équation *quartique* se résout à l'aide de multiples radicaux emboîtés.

(racines quadratiques et cubiques)

Alors... pourquoi l'équation du n-ième degré ne se résoudrait-elle pas aussi à l'aide de racines n-ième (et plus petites) ?

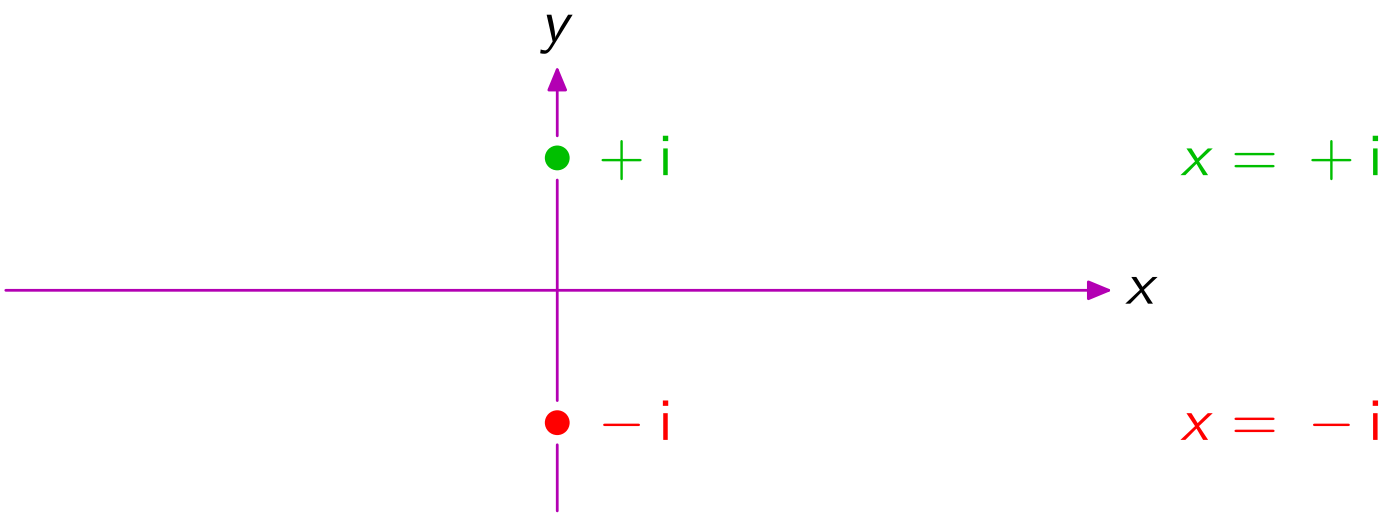
Pourquoi les clés les plus simples imaginables n'ouvriraient-elles pas toutes les portes du monde ? Espoir... naïf ! ! !

La théorie de Galois
est une théorie de *symétries non visuelles*, qui sont toutes pourtant des généralisations d'une symétrie géométrique (et donc visuelle) —
la conjugaison complexe :



Une symétrie des racines de $x^2 + 1 = 0$

Les deux racines « magiques » sont :



Racines dites « conjuguées »

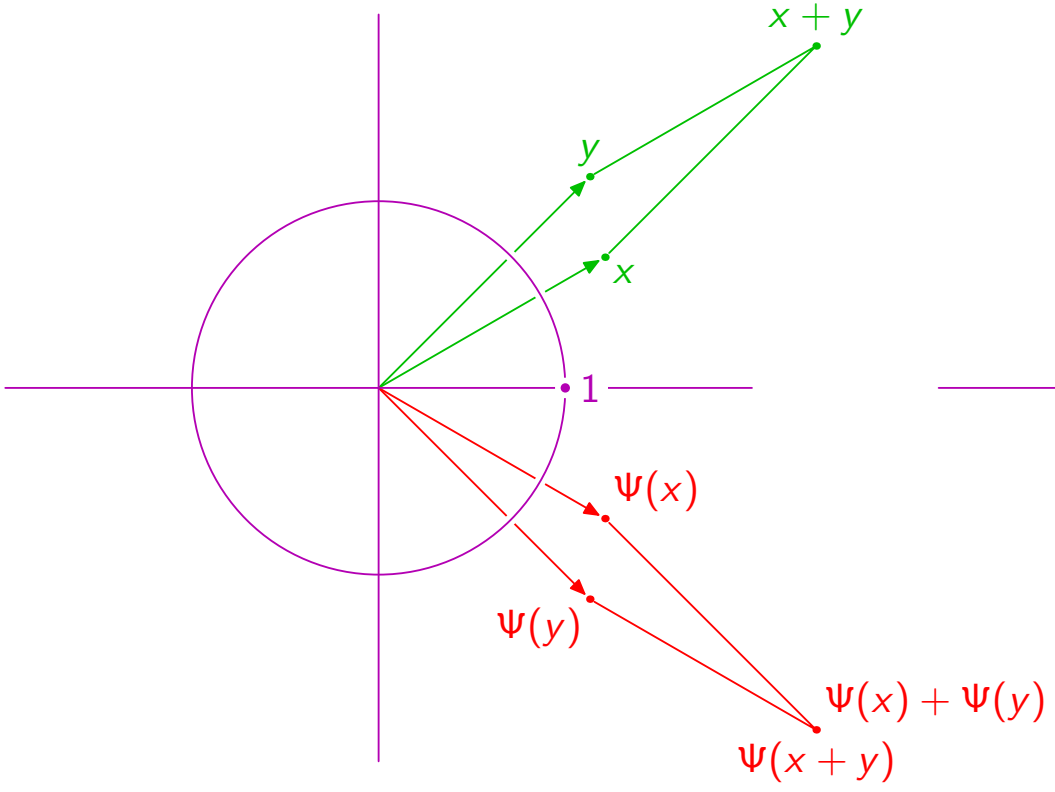
L'adjonction algébrique de i à $\mathbb{R}$ donne un corps dont l'élément générique est $a + b\,\mathrm{i}$

où a et b sont réels ($\in \mathbb{R}$)

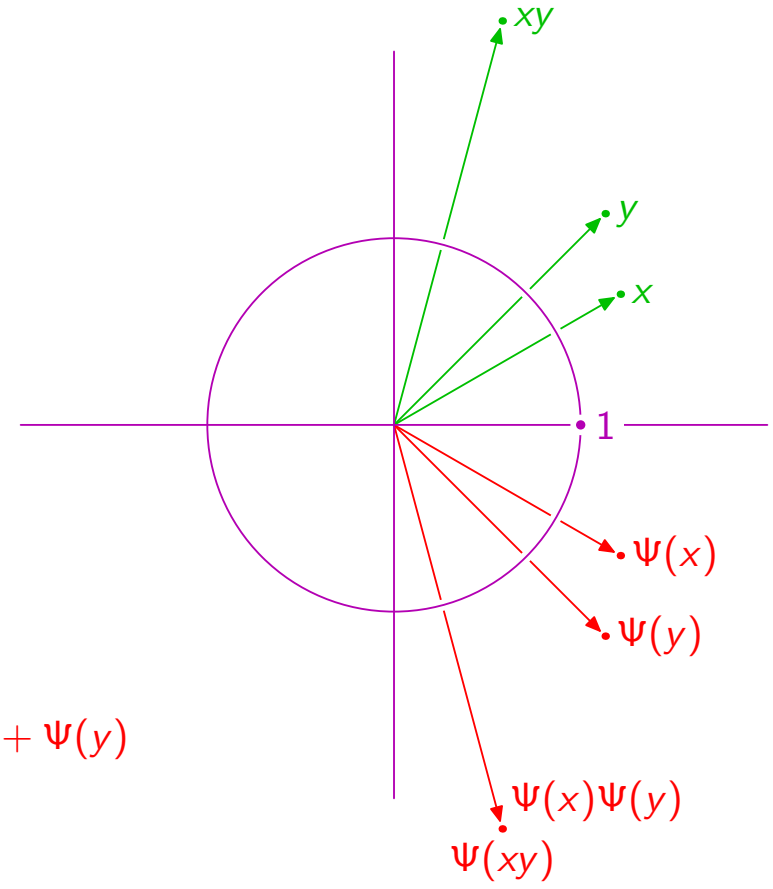
$\mathbb{C}$ est *bidimensionnel* par rapport à $\mathbb{R}$

Automorphisme du plan complexe $\mathbb{C}$ où tous les nombres réels restent fixes

(le sous corps $\mathbb{R}$ est invariant)



Addition



Multiplication

La conjugaison complexe Ψ respecte cette symétrie :

$$\boxed{+\mathrm{i}} : (a + \mathrm{i}\, b) + (c + \mathrm{i}\, d) = (a + c) + \mathrm{i}\,(b + d)$$

$$\Psi : \quad \updownarrow \qquad \updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$\boxed{-\mathrm{i}} : (a - \mathrm{i}\, b) + (c - \mathrm{i}\, d) = (a + c) - \mathrm{i}\,(b + d)$$

$$\boxed{\Psi(x) \quad + \quad \Psi(y) \quad = \quad \Psi(x + y)}$$

$$\boxed{+\mathrm{i}} : (a + \mathrm{i}\, b)\,(c + \mathrm{i}\, d) = (ac - bd) + \mathrm{i}\,(ad + bc)$$

$$\Psi : \quad \updownarrow \qquad \updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$\boxed{-\mathrm{i}} : (a - \mathrm{i}\, b)\,(c - \mathrm{i}\, d) = (ac - bd) - \mathrm{i}\,(ad + bc)$$

$$\boxed{\Psi(x)\Psi(y) \quad = \quad \Psi(xy)}$$

$\longleftarrow$

L'automorphisme $x + \mathrm{i}\, y \longmapsto x - \mathrm{i}\, y$ est *géométrique et visuel*

La théorie de Galois porte sur des symétries incroyablement *analogues* mais *pas du tout géométriques !*

Des symétries algébriques, formelles, toujours généralisations de la conjugaison complexe.

←

Notre première analogie avec la conjugaison complexe s'effectuera à partir d'un corps plus petit que $\mathbb{R}$, à savoir $\mathbb{Q}$ *(les nombres rationnels)*, sous-ensemble dense de la droite des réels.

Et qu'est-ce qu'un *corps* ?

Un ensemble de nombres avec 0 et 1,

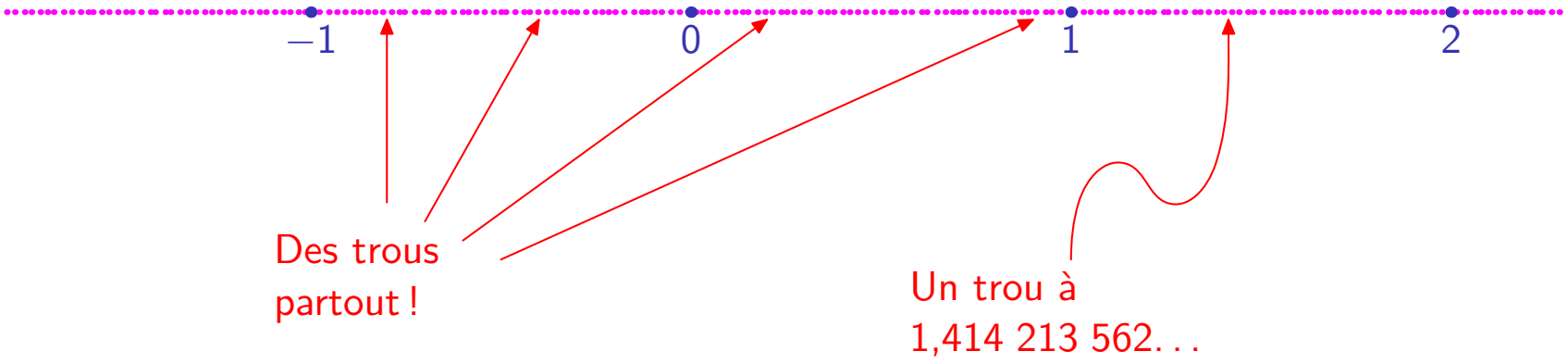
où

l'addition
la multiplication
la soustraction
la division

sont toujours possibles.

(sauf division par 0, bien sûr)

$\mathbb{Q}$:



Dense mais plein de trous !

Une symétrie des racines de $x^2 - 2 = 0$

Les deux racines « magiques » sont :

Racines dites « conjuguées »

L'adjonction algébrique de $\sqrt{2}$ à $\mathbb{Q}$ donne un corps dont l'élément générique est $a + b\sqrt{2}$

où a et b sont rationnels ($\in \mathbb{Q}$)

Le nouveau corps $\mathbb{Q}(\sqrt{2})$ est *bidimensionnel* par rapport à $\mathbb{Q}$

mais *tous ses éléments appartiennent à une seule droite*

On perd la qualité visuelle et géométrique.

La « conjugaison algébrique » Ψ respecte cette symétrie :

$$\boxed{+\sqrt{2}} : (a + \sqrt{2}\,b) + (c + \sqrt{2}\,d) = (a + c) + \sqrt{2}\,(b + d)$$

$$\Psi : \quad \updownarrow \qquad \updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$\boxed{-\sqrt{2}} : (a - \sqrt{2}\,b) + (c - \sqrt{2}\,d) = (a + c) - \sqrt{2}\,(b + d)$$

$$\boxed{\Psi(x) \quad + \quad \Psi(y) \quad = \quad \Psi(x + y)}$$

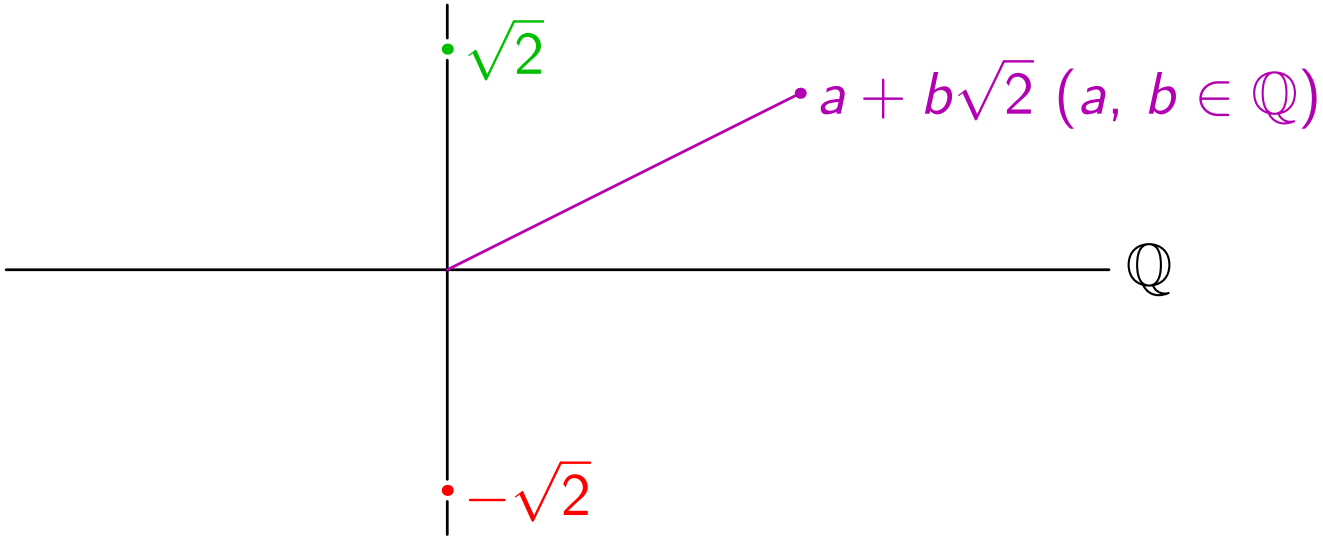
$$\boxed{+\sqrt{2}} : (a + \sqrt{2}\,b)\ (c + \sqrt{2}\,d) = (ac + 2bd) + \sqrt{2}\,(ad + bc)$$

$$\Psi : \quad \updownarrow \qquad \updownarrow \qquad \updownarrow \qquad \updownarrow$$

$$\boxed{-\sqrt{2}} : (a - \sqrt{2}\,b)\ (c - \sqrt{2}\,d) = (ac + 2bd) - \sqrt{2}\,(ad + bc)$$

$$\boxed{\Psi(x)\Psi(y) \quad = \quad \Psi(xy)}$$

Impossible de faire un « plan quadratique » analogue au plan complexe



qui respecte les distances des quantités $a + b\sqrt{2}$ dans la droite des réels

car il n'existe pas d'homéomorphisme (correspondance continue) entre deux espaces topologiques de dimensions différentes.

L'adjonction des racines d'une équation polynomiale à un corps « incomplet » (c'est-à-dire, il existe une équation qui n'est pas résoluble *dans* le corps, alors il faut y ajouter des « éléments magiques »)

Corps incomplet	Équation irrésoluble	Racines « magiques »	Corps étendu
$\mathbb{R}$	$x^2+1=0$	$\pm\,\mathrm{i}$	$\mathbb{R}(\mathrm{i})=\{x+\mathrm{i}\,y\}$ $x,\ y\in\mathbb{R}$
$\mathbb{Q}$	$x^2-2=0$	$\pm\sqrt{2}$	$\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\}$ $a,\ b\in\mathbb{Q}$

Les symétries de l'équation quartique $x^4 - x^2 - 2 = 0$

$$(x^2 - 2)(x^2 + 1) = 0$$

Les racines « magiques » sont :

$$x = \mathrm{i}$$

$$x = -\mathrm{i}$$

$$x = \sqrt{2}$$

$$x = -\sqrt{2}$$

Les éléments du corps étendu sont :

$$a + b\,\mathrm{i} + c\sqrt{2} + d\,\mathrm{i}\sqrt{2} \qquad \left[\text{Dim 4 par rapport à } \mathbb{Q}\right]$$

$$= (a + b\,\mathrm{i}) + (c + d\,\mathrm{i})\sqrt{2} \qquad \left[\text{Dim 2 par rapport à } \mathbb{Q}(\mathrm{i})\right]$$

$$= (a + c\sqrt{2}) + (b + d\sqrt{2})\,\mathrm{i} \qquad \left[\text{Dim 2 par rapport à } \mathbb{Q}(\sqrt{2})\right]$$

Un corps étendu est un *espace vectoriel* par rapport au corps de départ

Extension	Membre générique	Dimension
$\mathbb{R} \longrightarrow \mathbb{C}$	$x + \mathrm{i}\, y$ $(x,\ y \in \mathbb{R})$	2
$\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt{2})$	$a + b\sqrt{2}$ $(a,\ b \in \mathbb{Q})$	2
$\mathbb{Q} \longrightarrow \mathbb{Q}(\mathrm{i}, \sqrt{2})$	$a + b\,\mathrm{i} + c\sqrt{2} + d\,\mathrm{i}\sqrt{2}$ $(a,\ b,\ c,\ d \in \mathbb{Q})$	4

$$\begin{tikzcd}
 & K = \mathbb{Q}(i, \sqrt{2}) & \\
E = \mathbb{Q}(i) \arrow[ur, "\sqrt{2}"] & & \mathbb{Q}(\sqrt{2}) = F \arrow[ul, "i"'] \\
 & \mathbb{Q} \arrow[ul, "i"] \arrow[ur, "\sqrt{2}"'] &
\end{tikzcd}$$

$$\underbrace{\begin{aligned}[K : \mathbb{Q}] = 4 &= [K : E][E : \mathbb{Q}] = 2 \times 2 \\ &= [K : F][F : \mathbb{Q}] = 2 \times 2\end{aligned}}_{\text{Théorème des extensions itérées}}$$

Nous étendons l'analogie avec la conjugaison complexe au corps $\mathbb{Q}(\mathrm{i}, \sqrt{2})$,
corps de décomposition de l'équation quartique

$$x^4 - x^2 - 2 = 0.$$

$\longleftarrow$

Quelles sont les symétries du corps $\mathrm{K} = \mathbb{Q}(\mathrm{i}, \sqrt{2})$?

Deux types de « conjugaison » :

$\mathrm{V}: \quad +\mathrm{i} \quad \leftrightarrow \quad -\mathrm{i}$ (i et $-$i sont indifférenciables)

$\mathrm{H}: \quad +\sqrt{2} \quad \leftrightarrow \quad -\sqrt{2}$ ($\sqrt{2}$ et $-\sqrt{2}$ sont indifférenciables)

$$\mathrm{V}(a + b\,\mathrm{i} + c\sqrt{2} + d\,\mathrm{i}\sqrt{2}) = a - b\,\mathrm{i} + c\sqrt{2} - d\,\mathrm{i}\sqrt{2}$$

$$\mathrm{H}(a + b\,\mathrm{i} + c\sqrt{2} + d\,\mathrm{i}\sqrt{2}) = a + b\,\mathrm{i} - c\sqrt{2} - d\,\mathrm{i}\sqrt{2}$$

Mais il y a aussi le « produit » des deux types de conjugaison

$$\Pi = \mathrm{HV} = \mathrm{VH}$$

$$\Pi(a + b\,\mathrm{i} + c\sqrt{2} + d\,\mathrm{i}\sqrt{2}) = a - b\,\mathrm{i} - c\sqrt{2} + d\,\mathrm{i}\sqrt{2}$$

Une troisième « conjugaison » dans K.

←

L'analogie révolutionnaire de Galois :

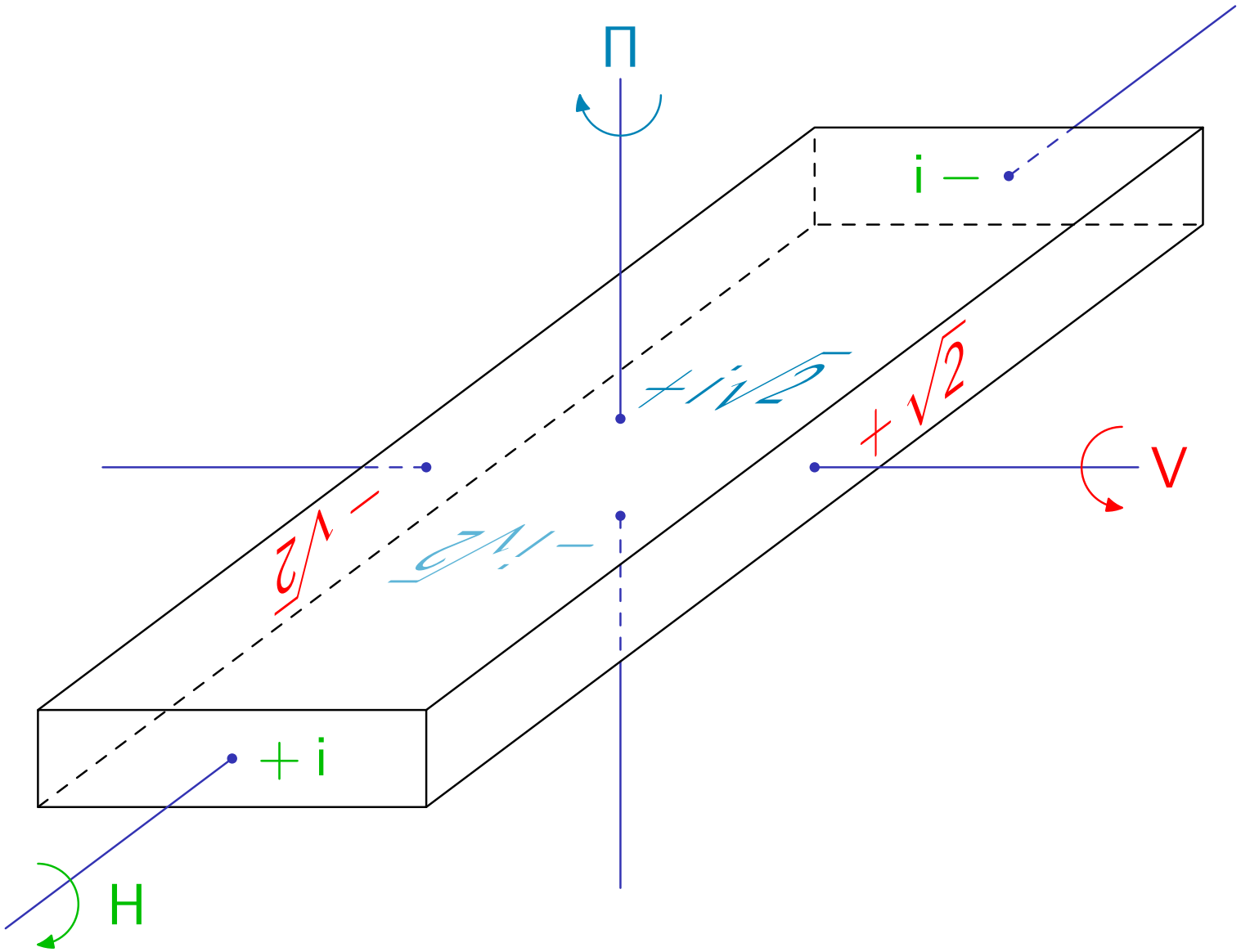
Il traite les automorphismes
comme s'ils étaient des nombres.

Il construit une « table de multiplication » pour eux.

Résumé des symétries de $K = \mathbb{Q}(\,i\,,\sqrt{2})$

	I	V	H	Π
I	I	V	H	Π
V	V	I	Π	H
H	H	Π	I	V
Π	Π	H	V	I

3 types non triviaux de « conjugaison algébrique »
et un type trivial (I)



Le groupe de Klein G_K :
les symétries d'une (algé)brique

←

Deuxième analogie révolutionnaire de Galois :

Il traite les groupes et leurs sous-groupes comme s'ils étaient des nombres.

Il invente une sorte de « division » pour ces grandes structures abstraites.

La structure à gros grain de G_K

On a « divisé » G_K par son sous-groupe (distingué) $\{I, V\}$ pour obtenir un *groupe quotient*

	I V	H Π
sous-groupe I V	IV	HΠ
classe latérale H Π	HΠ	IV

Isomorphe à $\mathbb{Z}_2$:

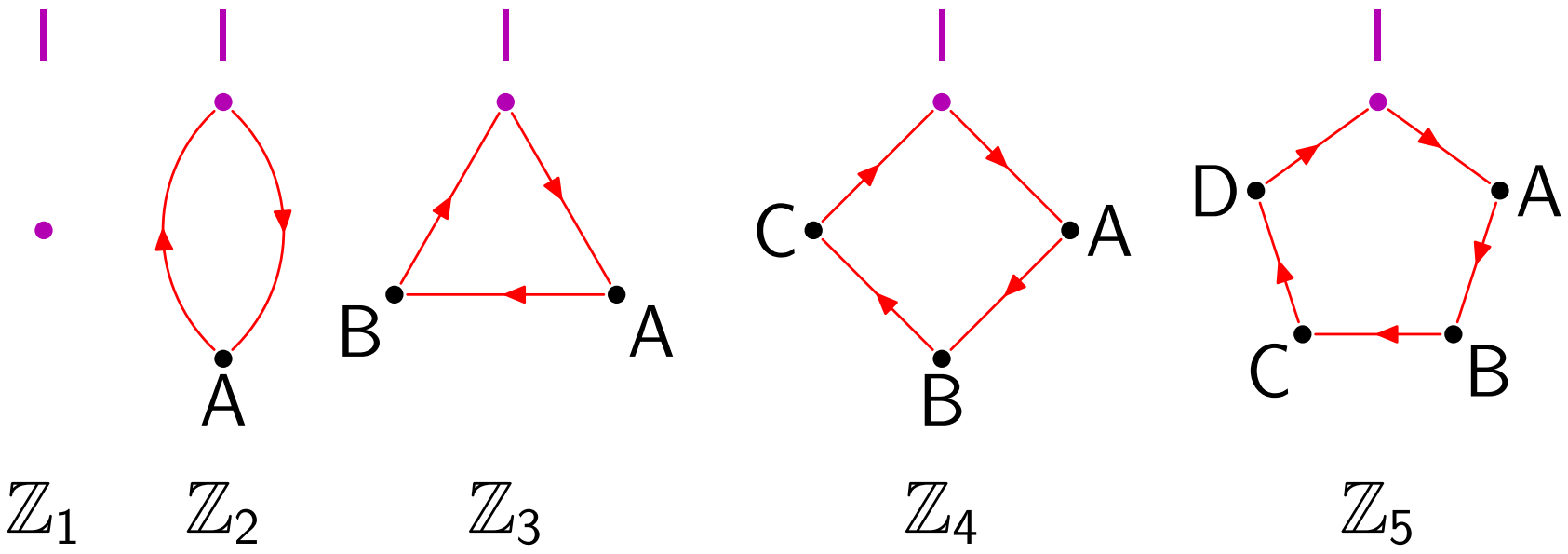
	0	1
0	0	1
1	1	0

le groupe cyclique d'ordre 2

Les diagrammes de Cayley rendent visibles et tangibles les groupes.

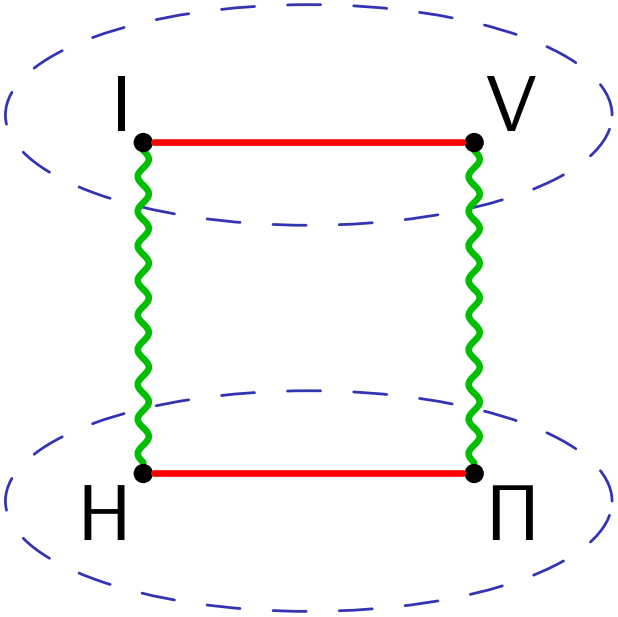
Les groupes cycliques $\mathbb{Z}_n$

Diagrammes de Cayley



Pour p premier, $\mathbb{Z}_p$ n'a pas de sous-groupe propre

Diagramme de Cayley du groupe de Klein G_K



sous-groupe $\{I, V\}$

classe latérale de $\{I, V\}$

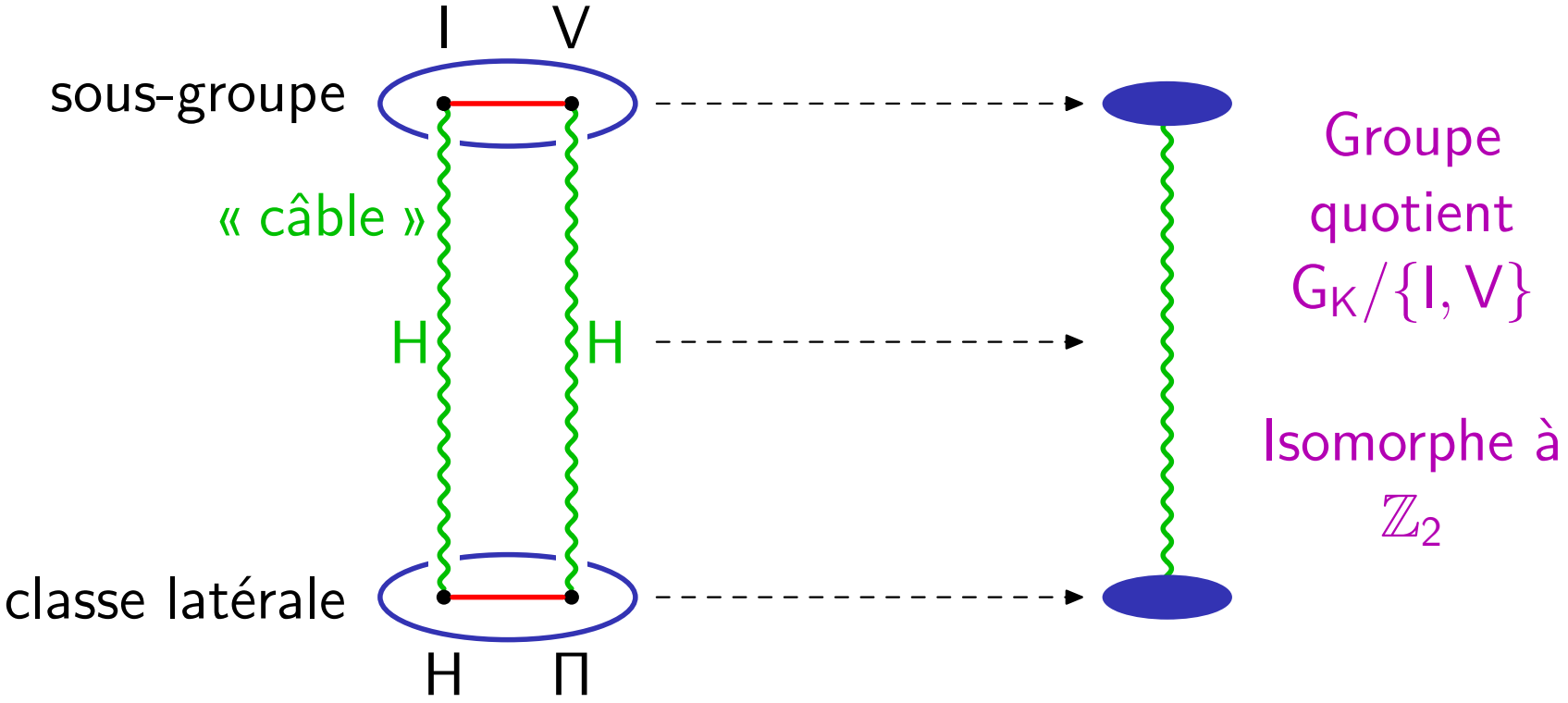
←

La visualisation du concept abstrait de « groupe quotient » à l'aide des diagrammes de Cayley.

Le rôle critique des « câbles » qui relient les sous-structures dans les diagrammes.

« Classe latérale » : sous-groupe multiplié par un élément du groupe.

La structure à gros grain de G_K

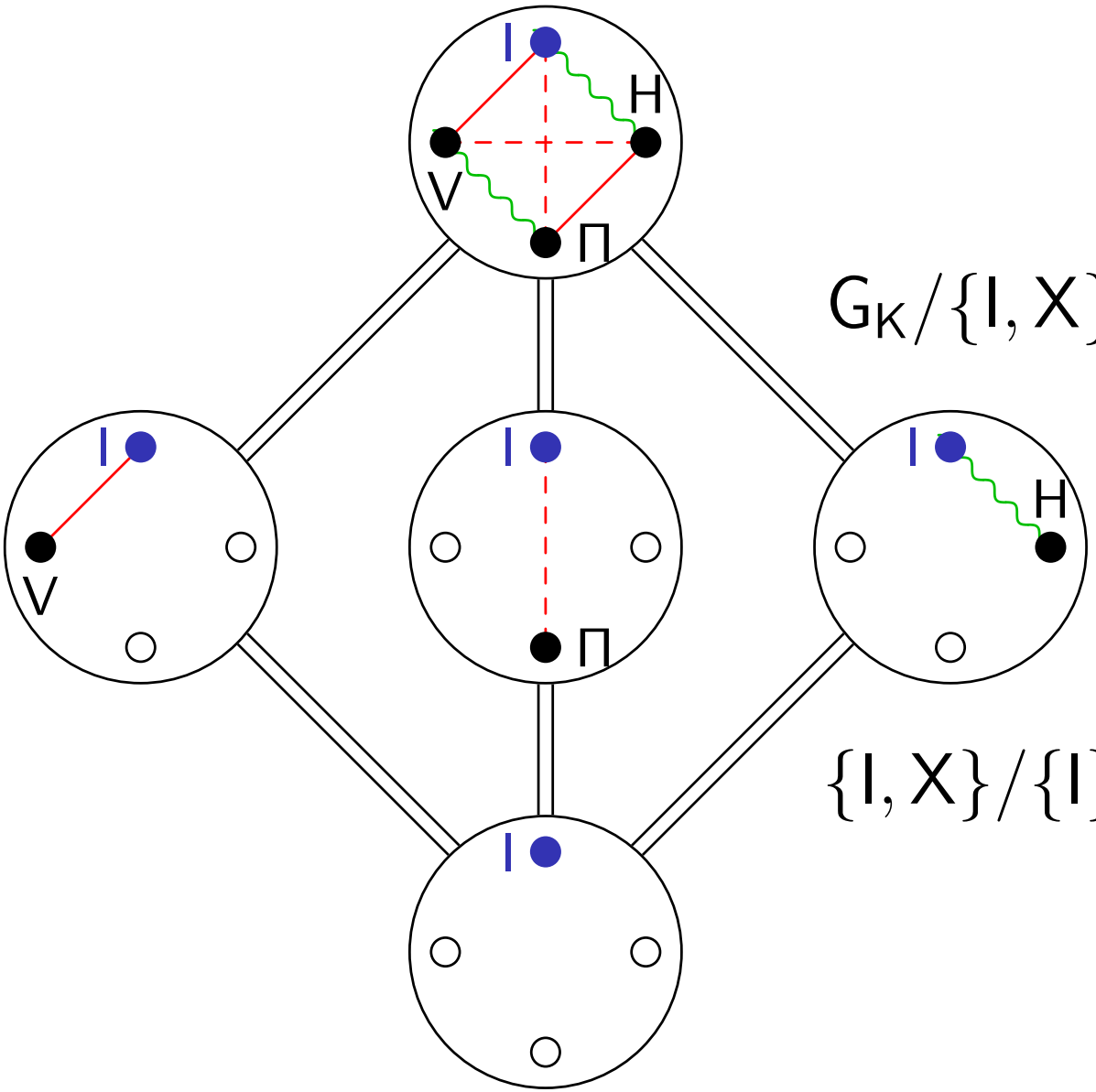


Troisième analogie révolutionnaire de Galois :

Il crée deux treillis de structures totalement différentes

et en observe l'isomorphie parfaite !

Le treillis des sous-groupes de G_K



$G_K/\{I, X\} \sim \mathbb{Z}_2$

$\{I, X\}/\{I\} \sim \mathbb{Z}_2$

Le treillis des extensions de corps entre $\mathbb{Q}$ et $\mathbb{Q}(\mathrm{i}, \sqrt{2})$

$$
\begin{tikzcd}
 & \mathbb{Q}(\mathrm{i}, \sqrt{2}) \arrow[dl, equal, "-\mathrm{i}\sqrt{2}"'] \arrow[d, equal, "-\sqrt{2}"'] \arrow[dr, equal, "-\mathrm{i}"] & \\
\mathbb{Q}(\mathrm{i}) \arrow[dr, equal, "-\mathrm{i}"'] & \mathbb{Q}(\mathrm{i}\sqrt{2}) \arrow[d, equal, "-\mathrm{i}\sqrt{2}"'] & \mathbb{Q}(\sqrt{2}) \arrow[dl, equal, "\sqrt{2}"] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Extensions galoisiennes de $\mathbb{Q}(x)$

Extensions galoisiennes de $\mathbb{Q}$

←

Le cas révélateur de l'équation cubique

Si une équation *quadratique* a *deux*
« conjugaisons algébriques » (Ψ et I)
et une équation *quartique* en a *quatre* (I, V, H, Π),
alors combien pour une *cubique* ?

Non, pas trois ! Six !

$\longleftarrow$

Pourquoi six ?

Parce que $(x-a)(x-b)(x-c)=0$
devient partiellement résoluble
si on ajoute $\underbrace{a}_{\uparrow}$ à $\mathbb{Q}$

(élément de degré 3)

L'équation se factorise dans $\mathbb{Q}(a)$:

$$(x-a)\Big[(x-b)(x-c)\Big]=0$$

Il reste une équation quadratique, et pour tout résoudre, il faut ajouter soit $\underbrace{b}_{\uparrow}$ soit $\underbrace{c}_{\uparrow}$

(éléments de degré 2)

Alors, en tout, $3\times 2=6$

Les six symétries de l'équation cubique $x^3 - 2 = 0$

Les trois racines sont χ, Ξ, Θ

$$\chi = \sqrt[3]{2} \simeq 1{,}259\ 921\ \ldots$$

$$x^3 - 2 = (x - \chi)(x^2 + \chi x + \chi^2)$$

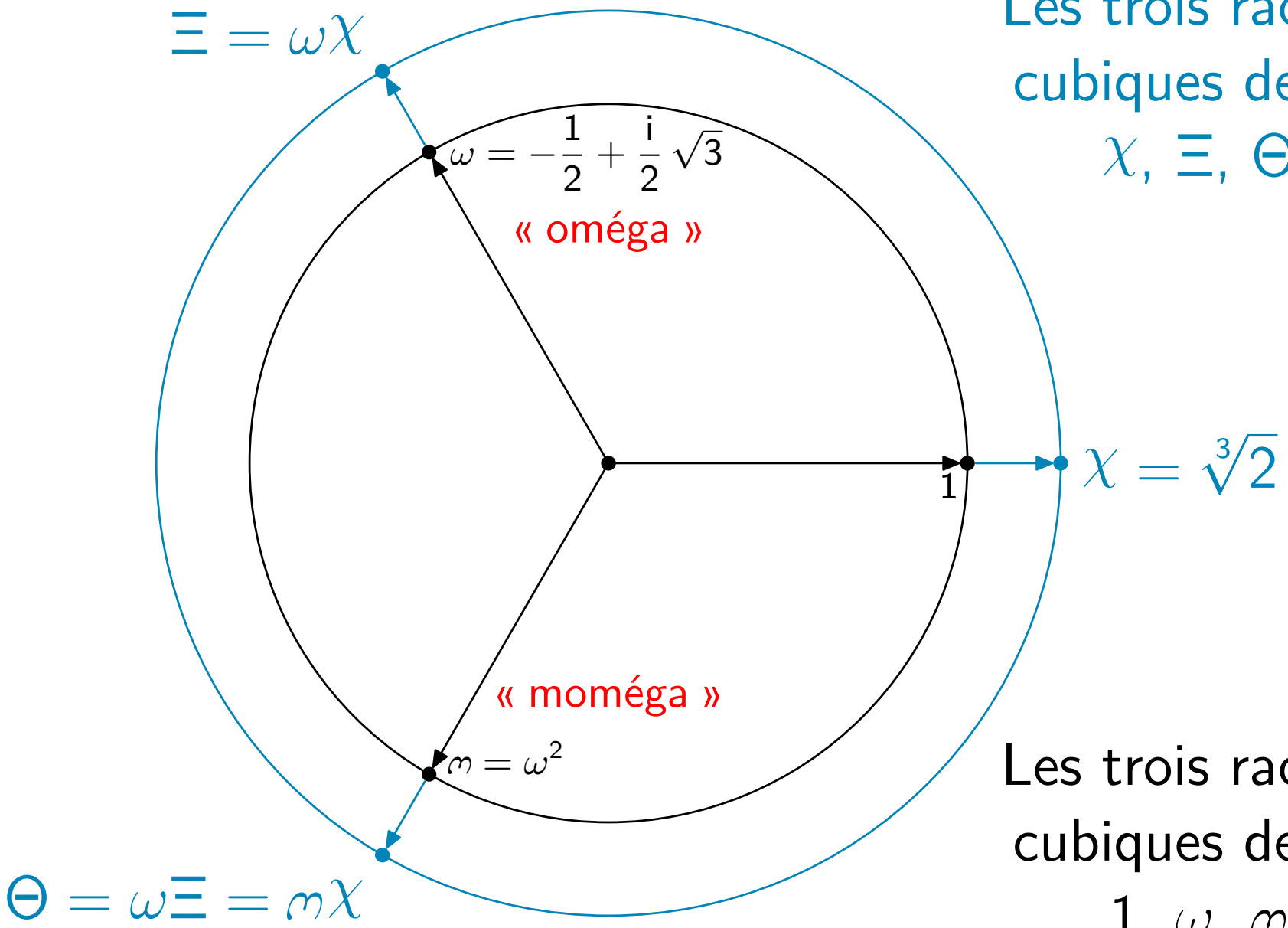
Il reste une équation quadratique à résoudre :

$$x^2 + \chi x + \chi^2 = 0$$

Les deux racines sont : $\begin{array}{rcl} \Xi & = & \omega\chi \\ \Theta & = & \omega^2\chi \end{array}$

où $\omega = -\dfrac{1}{2} + \dfrac{\mathrm{i}}{2}\sqrt{3}$ (racine cubique de 1)

Les trois racines cubiques de 2 : χ, Ξ, Θ



Les trois racines cubiques de 1 : 1, ω, $\mathcal{m}$

K = le corps de décomposition du polynôme $x^3 - 2$ créé par deux extensions de $\mathbb{Q}$

$$
\begin{tikzcd}
\mathrm{K} = \mathbb{Q}(\chi, \omega) = \mathrm{U}(\omega) \\
\mathrm{U} = \mathbb{Q}(\chi) \arrow[u, "\omega = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}"'] \\
\mathbb{Q} \arrow[u, "\chi = \sqrt[3]{2}"']
\end{tikzcd}
$$

6 = 2 × 3

Élément générique de K :

$$u + v\omega \quad (u,\ v \in \mathrm{U})$$

[K a dim 2 par rapport à U ; 6 par rapport à $\mathbb{Q}$]

Élément générique de U :

$$a + b\chi + c\chi^2 \quad (a,\ b,\ c \in \mathbb{Q})$$

[U a dim 3 par rapport à $\mathbb{Q}$]

K = le corps de décomposition du polynôme $x^3 - 2$ créé par deux extensions *différentes* de $\mathbb{Q}$

$$\begin{tikzcd}
\mathrm{K} = \mathbb{Q}(\omega, \chi) = \mathrm{W}(\chi) \\
\mathrm{W} = \mathbb{Q}(\omega) \arrow[u, "\chi"'] \\
\mathbb{Q} \arrow[u, "\omega"']
\end{tikzcd}$$

$6 \left\{ \begin{array}{l} 3 \left\{ \mathrm{K} \to \mathrm{W} \right. \\ 2 \left\{ \mathrm{W} \to \mathbb{Q} \right. \end{array} \right.$

Élément générique de K :

$w + x\chi + y\chi^2 \quad (w,\ x,\ y \in \mathrm{W})$

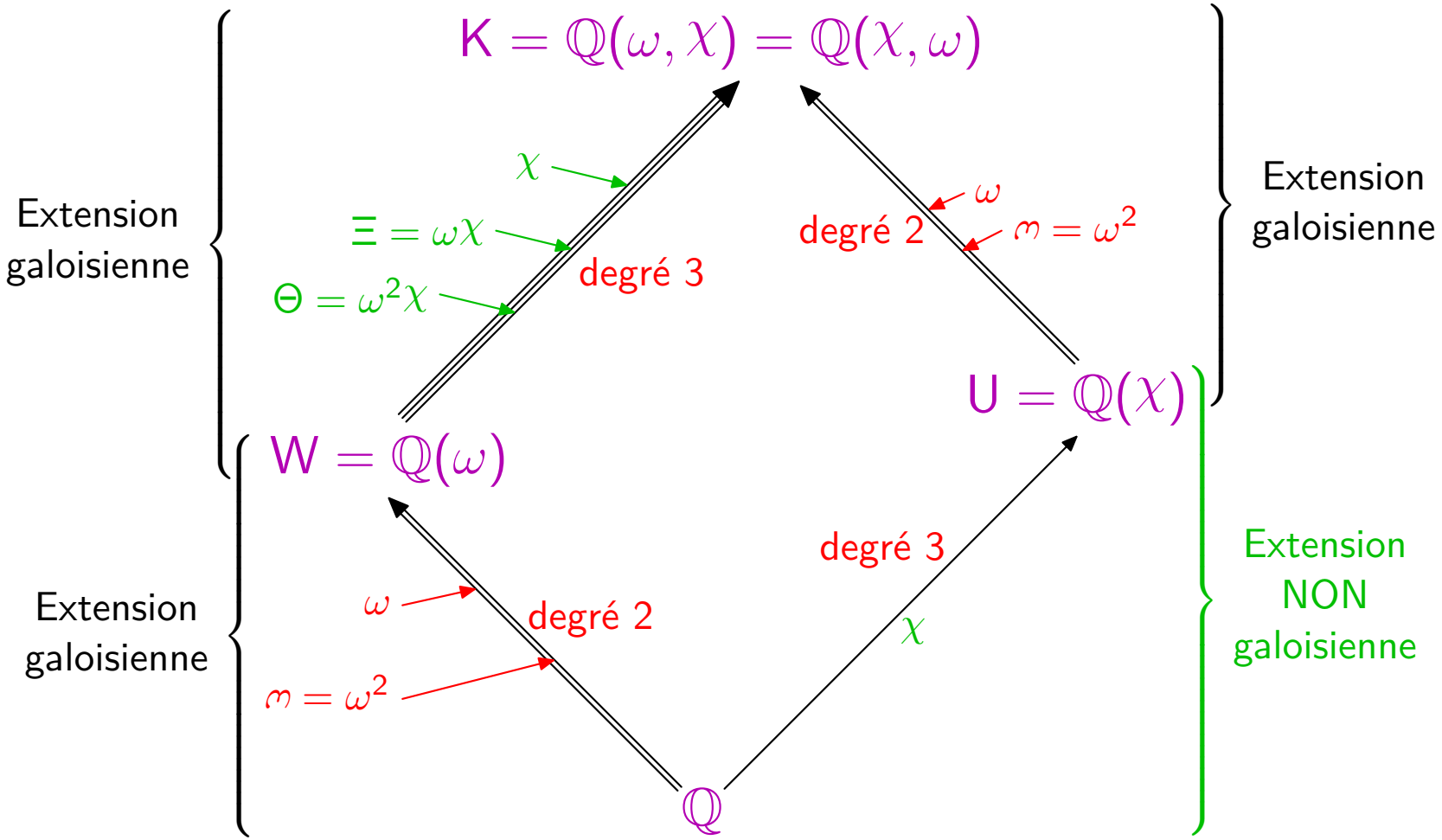
[K a dim 3 par rapport à W ; 6 par rapport à $\mathbb{Q}$]

Élément générique de W :

$a + b\omega \quad (a,\ b \in \mathbb{Q})$

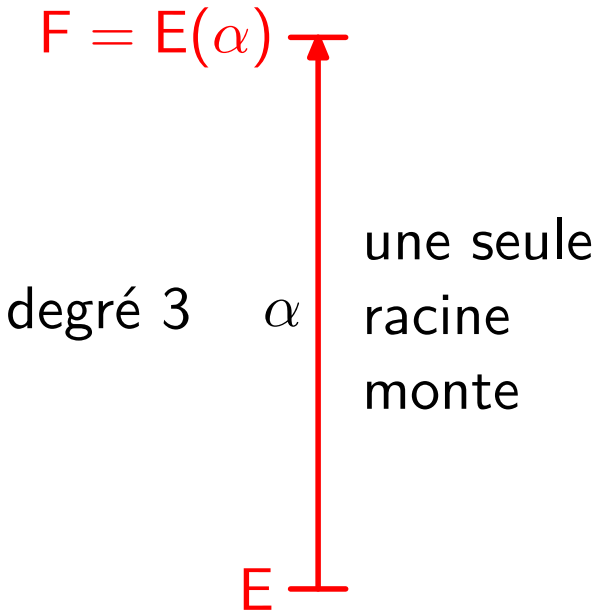
[W a dim 2 par rapport à $\mathbb{Q}$]

Le corps de décomposition de $x^3 - 2$

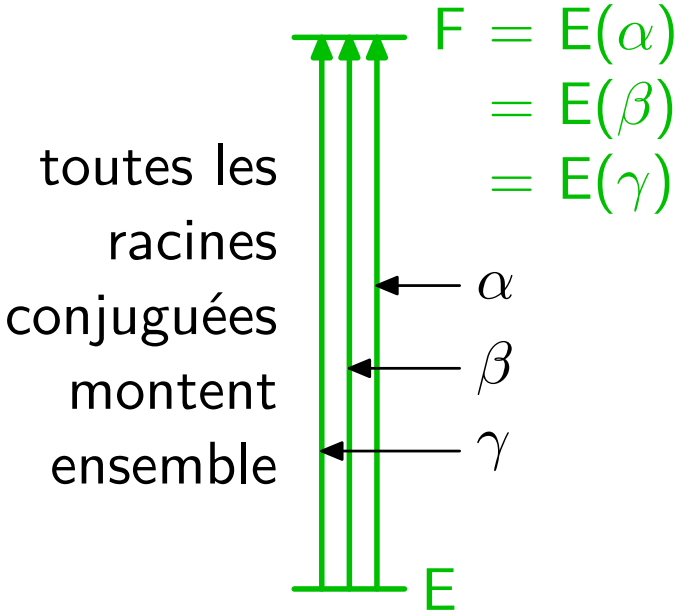


Qu'est-ce qu'une extension galoisienne ?

C'est une extension où
toutes les racines conjuguées montent ensemble



Extension NON galoisienne

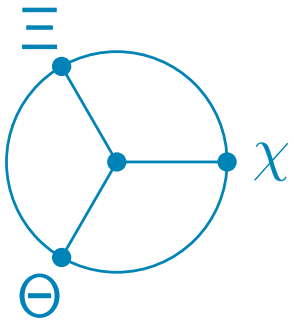


Extension galoisienne

Les extensions conjuguées

Ce qu'on a fait pour χ, on aurait pu en faire autant pour Ξ ou pour Θ, les *racines conjuguées* de χ.

Les 3 racines de $x^3 - 2$



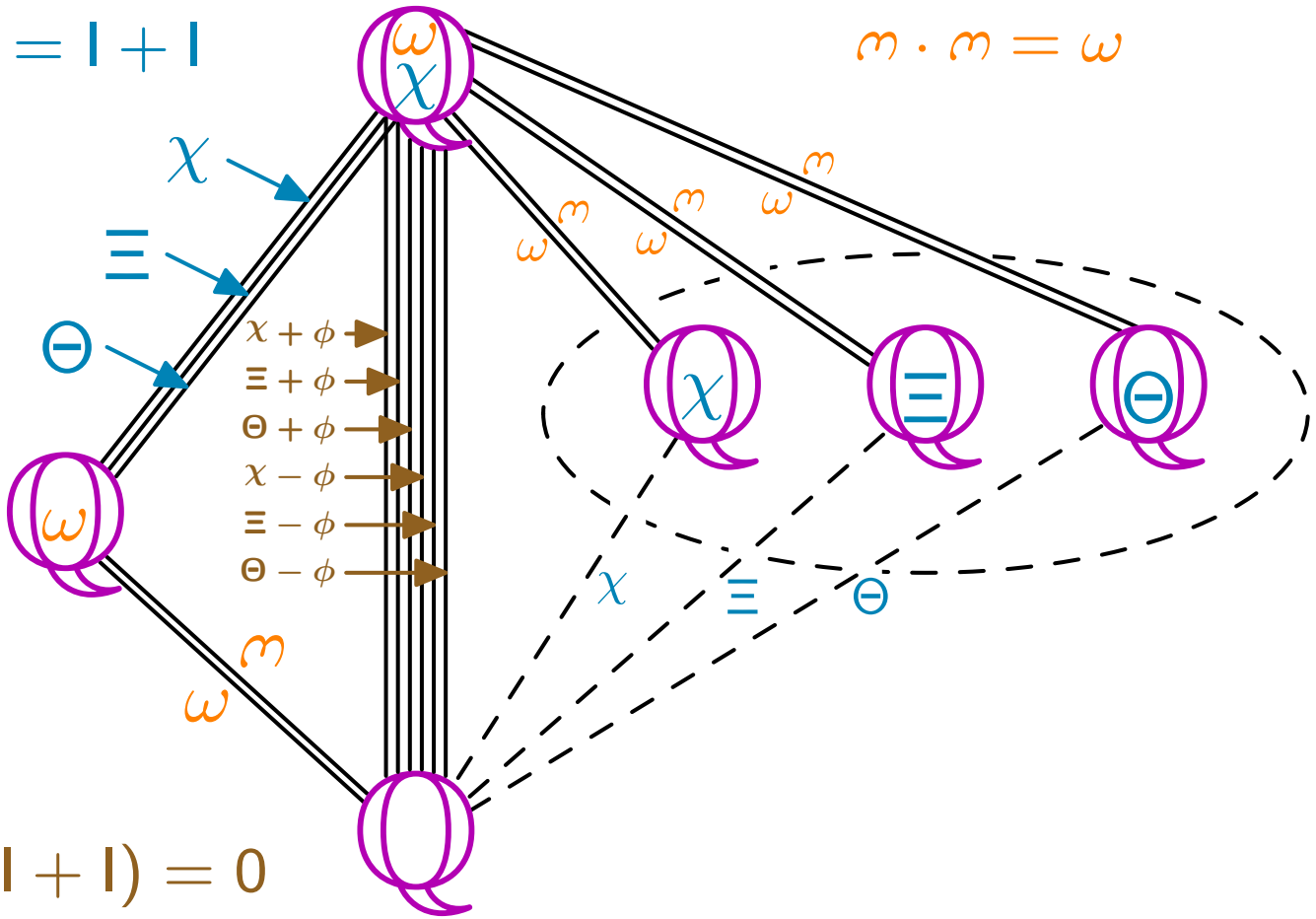
$$\begin{tikzcd}
 & K & \\
 & \mathbb{Q}(\chi) \arrow[u, Rightarrow, "\omega"] & \\
\mathbb{Q}(\omega) \arrow[uur, Rightarrow, "\text{Ext. gal.}"', "\chi"] & \mathbb{Q}(\Xi) \arrow[uu, Rightarrow, "\omega"] & \\
 & \mathbb{Q}(\Theta) \arrow[uuu, Rightarrow, "\omega"] & \\
 & \mathbb{Q} \arrow[ul, Rightarrow, "\omega", "\text{Ext. gal.}"'] \arrow[uu, "\chi"] \arrow[uur, "\Xi"] \arrow[uuur, "\Theta"] &
\end{tikzcd}$$

Extensions gal.

Extensions NON galoisiennes, extensions *conjuguées* de $\mathbb{Q}$; elles sont toutes isomorphes (indifférenciables)

$$\chi \cdot \chi \cdot \chi =$$
$$\Xi \cdot \Xi \cdot \Xi =$$
$$\Theta \cdot \Theta \cdot \Theta = \mathsf{I} + \mathsf{I}$$

$$\omega \cdot \omega \cdot \omega = \mathsf{I} = \mathfrak{m} \cdot \mathfrak{m} \cdot \mathfrak{m}$$
$$\omega \cdot \omega = \mathfrak{m}$$
$$\mathfrak{m} \cdot \mathfrak{m} = \omega$$



$$\phi \cdot \phi + (\mathsf{I} + \mathsf{I} + \mathsf{I}) = 0$$

Pour une cubique générale avec coefficients rationnels, les racines ont la forme

$$\sqrt[3]{r+\sqrt{\Delta}}+\sqrt[3]{r-\sqrt{\Delta}}$$

où r et Δ sont rationnels, et sont fonctions des coefficients du polynôme cubique.
On a donc affaire, en général, à une extension *quadratique* (par $\sqrt{\Delta}$) et aussi une extension *cubique* (par $\sqrt[3]{\ldots}$)
ce qui fait que le corps de décomposition d'une cubique a, en général, une dimension de **6** par rapport à $\mathbb{Q}$.

$\longleftarrow$

Les symétries du corps $\mathsf{K} = \mathbb{Q}(\chi, \Xi, \Theta) = \mathbb{Q}(\chi, \omega)$

« f » : $\Xi \longleftrightarrow \Theta \quad [\omega \longleftrightarrow \mathcal{M}]$

« P » : $\chi \longrightarrow \Xi \longrightarrow \Theta$

Automorphismes du corps K en tenant fixe le corps $\mathbb{Q}$:

Généralisations de la conjugaison complexe.

Pourquoi y a-t-il des symétries d'une cubique ?

Parce que les racines sont indifférenciables algébriquement.

Pourquoi ça ?

Parce que

$$(x-a)(x-b)(x-c)=0$$

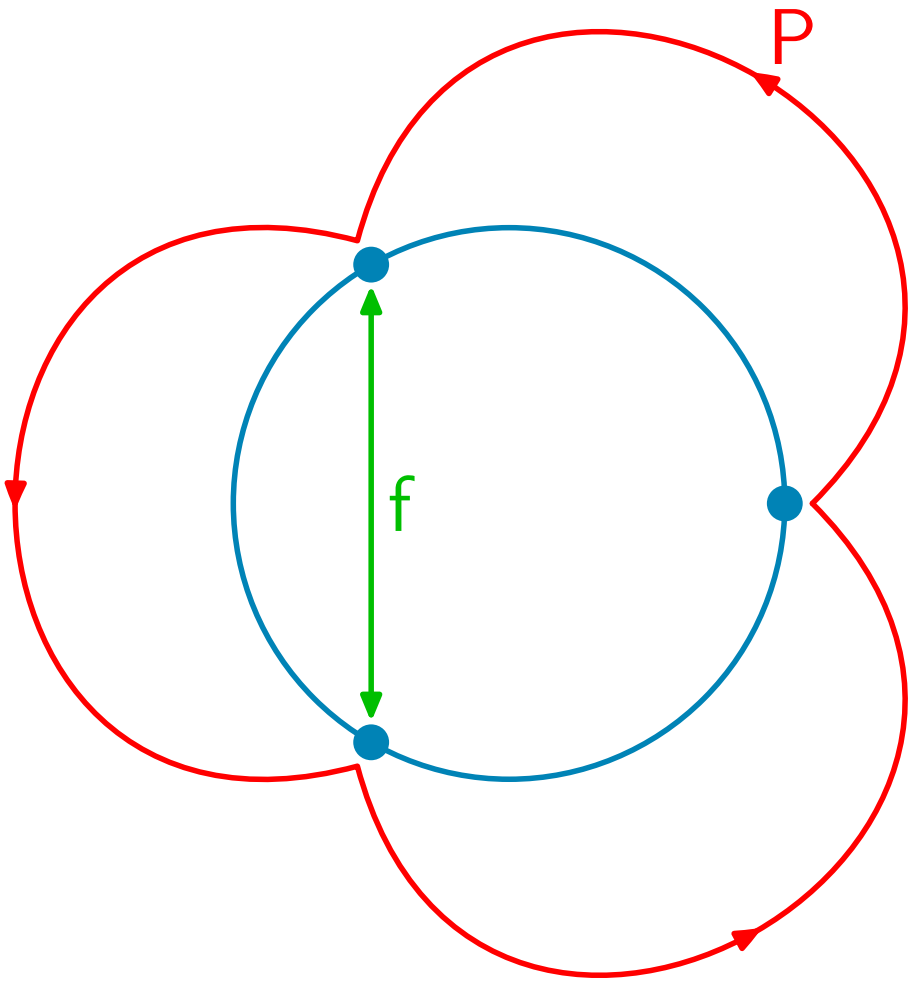
devient

$$x^3-\underbrace{(a+b+c)}x^2+\underbrace{(ab+bc+ca)}x-\underbrace{(abc)}=0$$

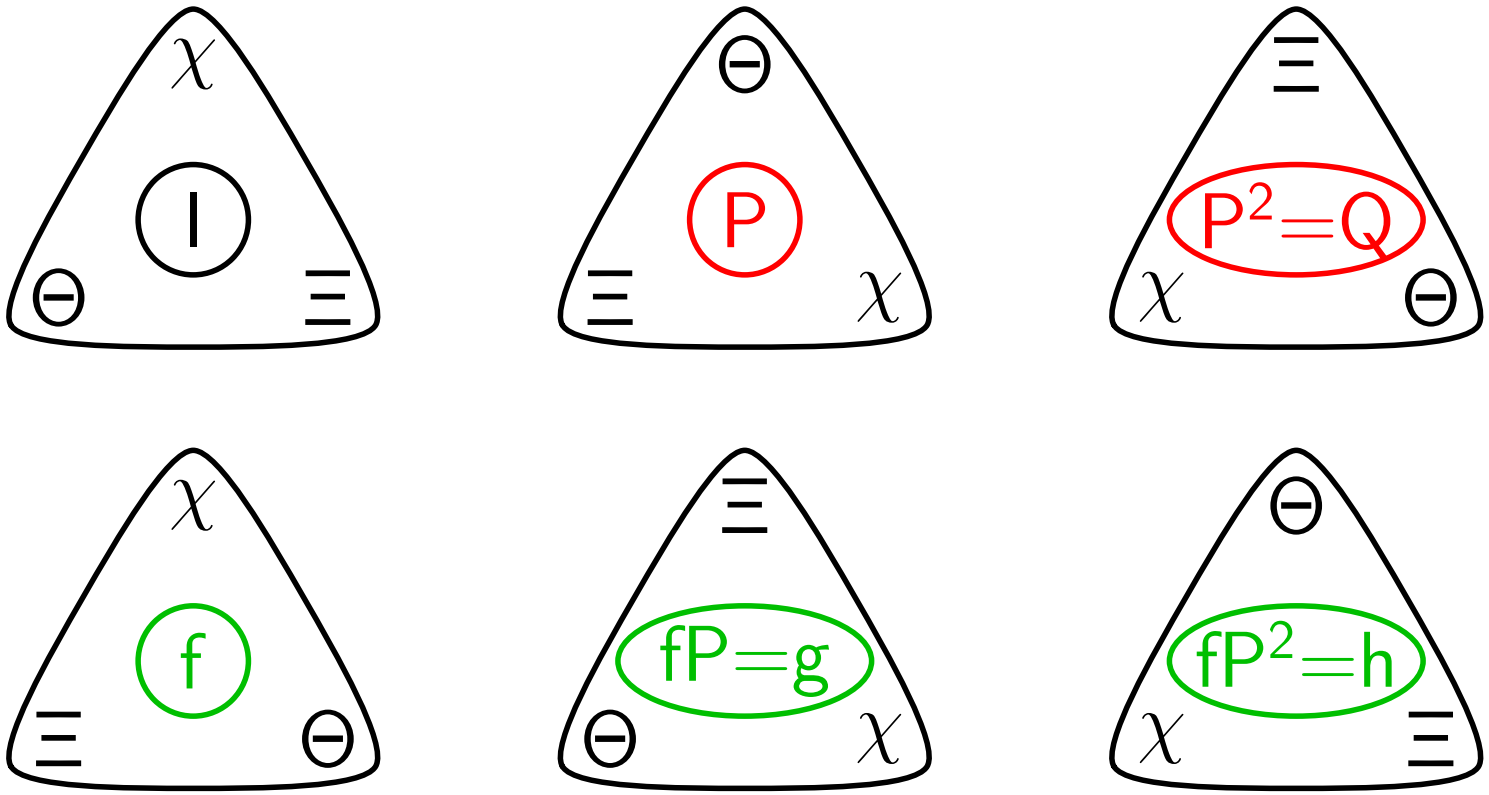
Invariant pour

$$a \leftrightarrow b$$
$$b \leftrightarrow c$$
$$c \leftrightarrow a$$
$$a \to b \to c$$
$$a \leftarrow b \leftarrow c$$

←



Un échange (f) et une rotation cyclique (P) suffisent pour générer toutes les permutations possibles de 3 objets (χ, Ξ, Θ) — à savoir, 6.



$f : \Xi \longleftrightarrow \Theta$ $\qquad$ $g : \chi/\Xi$ $\qquad$ $h : \chi/\Theta$

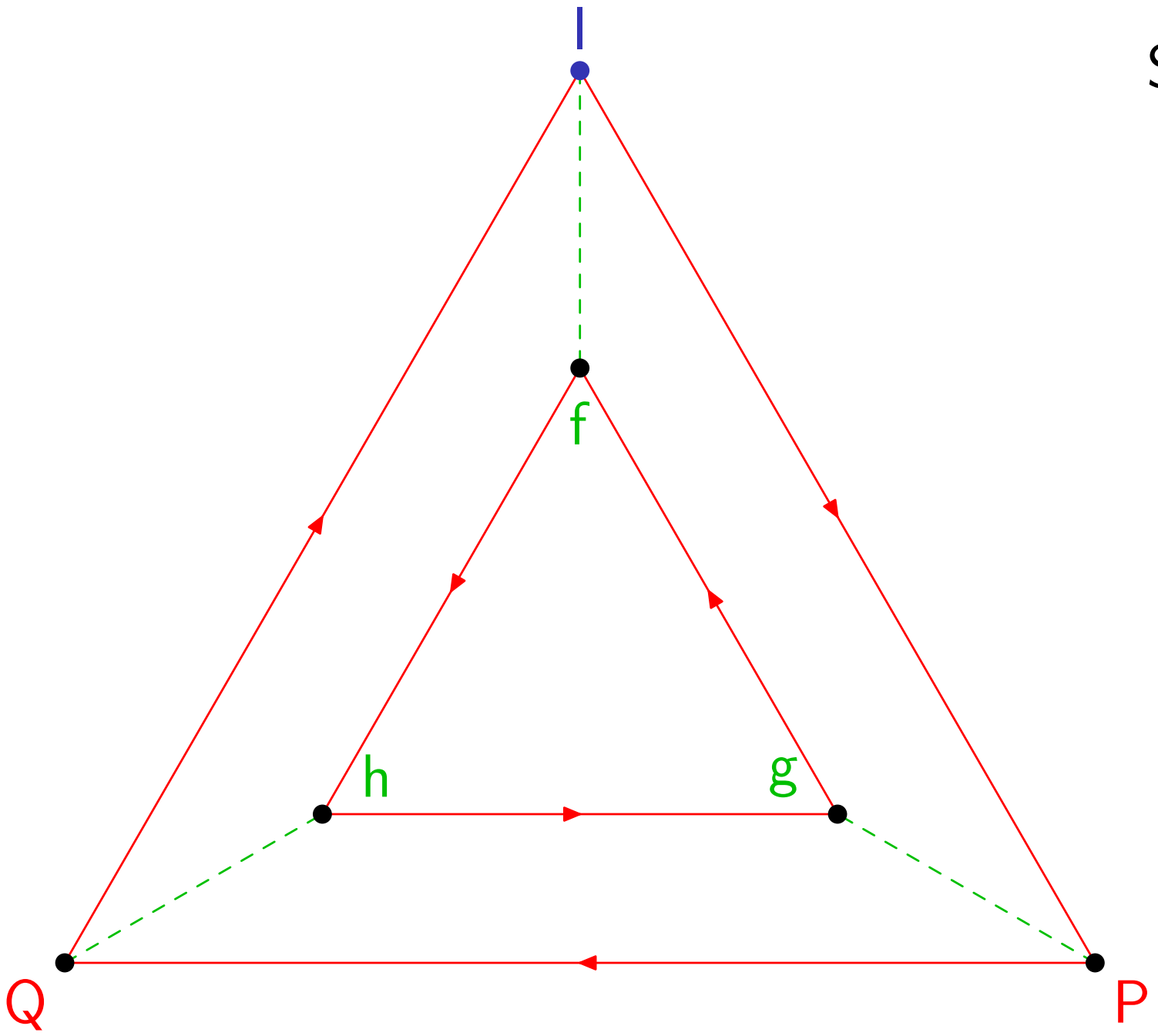
$P : \chi \longrightarrow \Xi \longrightarrow \Theta$ $\qquad$ $Q = P^{-1} = P^2$

Le groupe S_3 des permutations de 3 objets

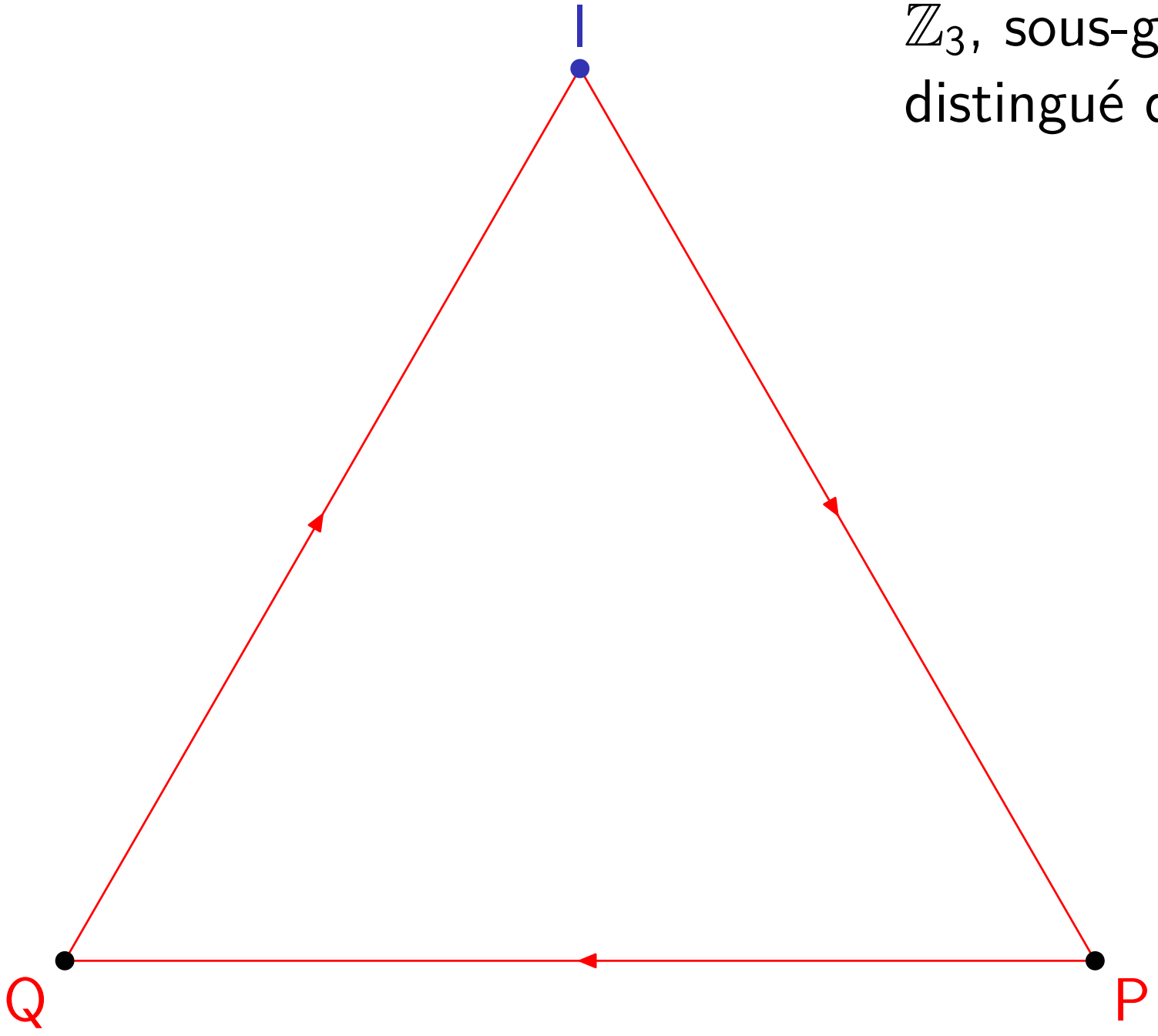
		I	P	Q	f	g	h
sous-groupe	I	I	P	Q	f	g	h
	P	P	Q	I	g	h	f
	Q	Q	I	P	h	f	g
classe latérale	f	f	h	g	I	Q	P
	g	g	f	h	P	I	Q
	h	h	g	f	Q	P	I

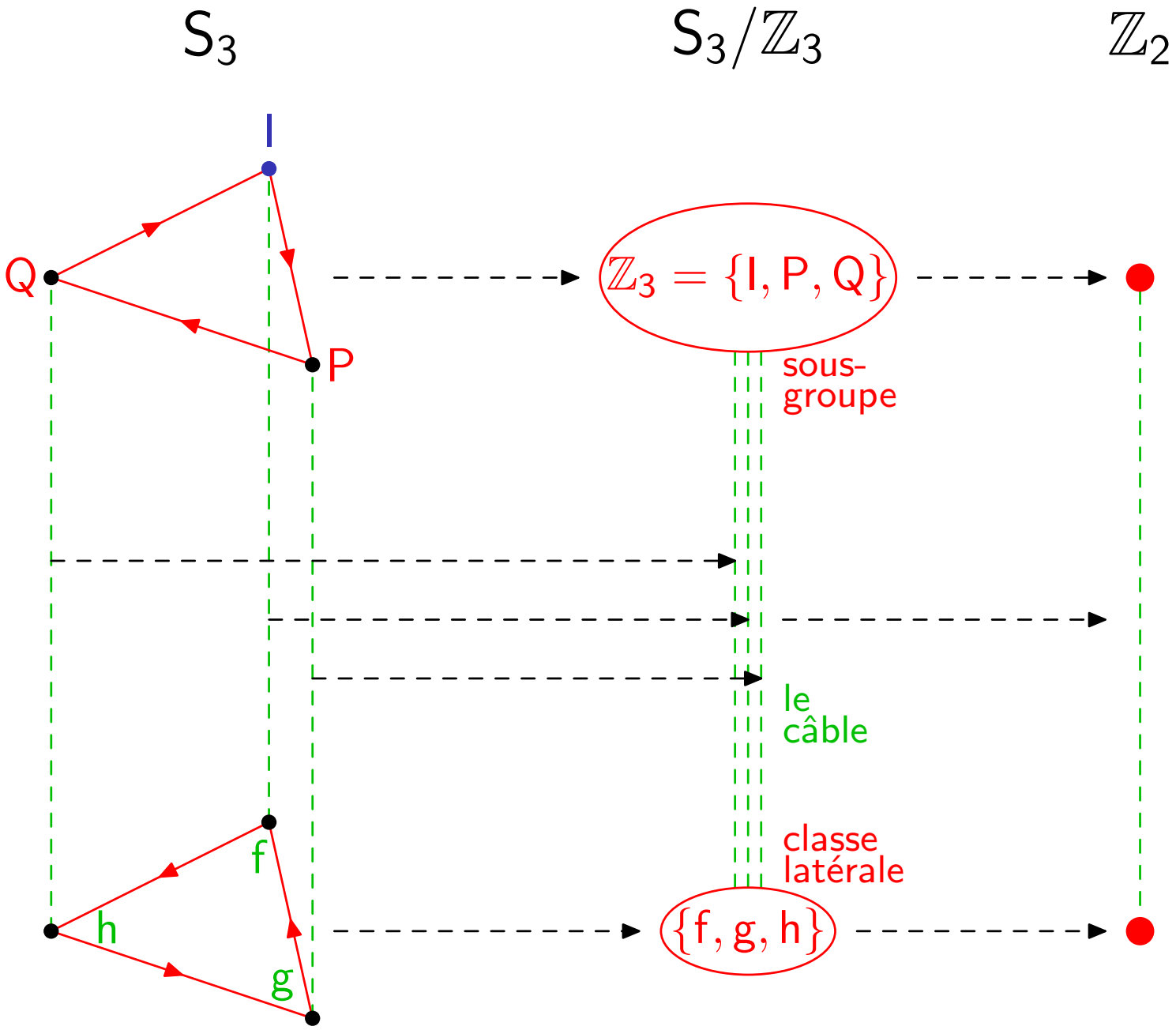
Le groupe quotient $S_3/\{I, P, Q\} \sim \mathbb{Z}_2$

S_3



$\mathbb{Z}_3$, sous-groupe distingué de S_3



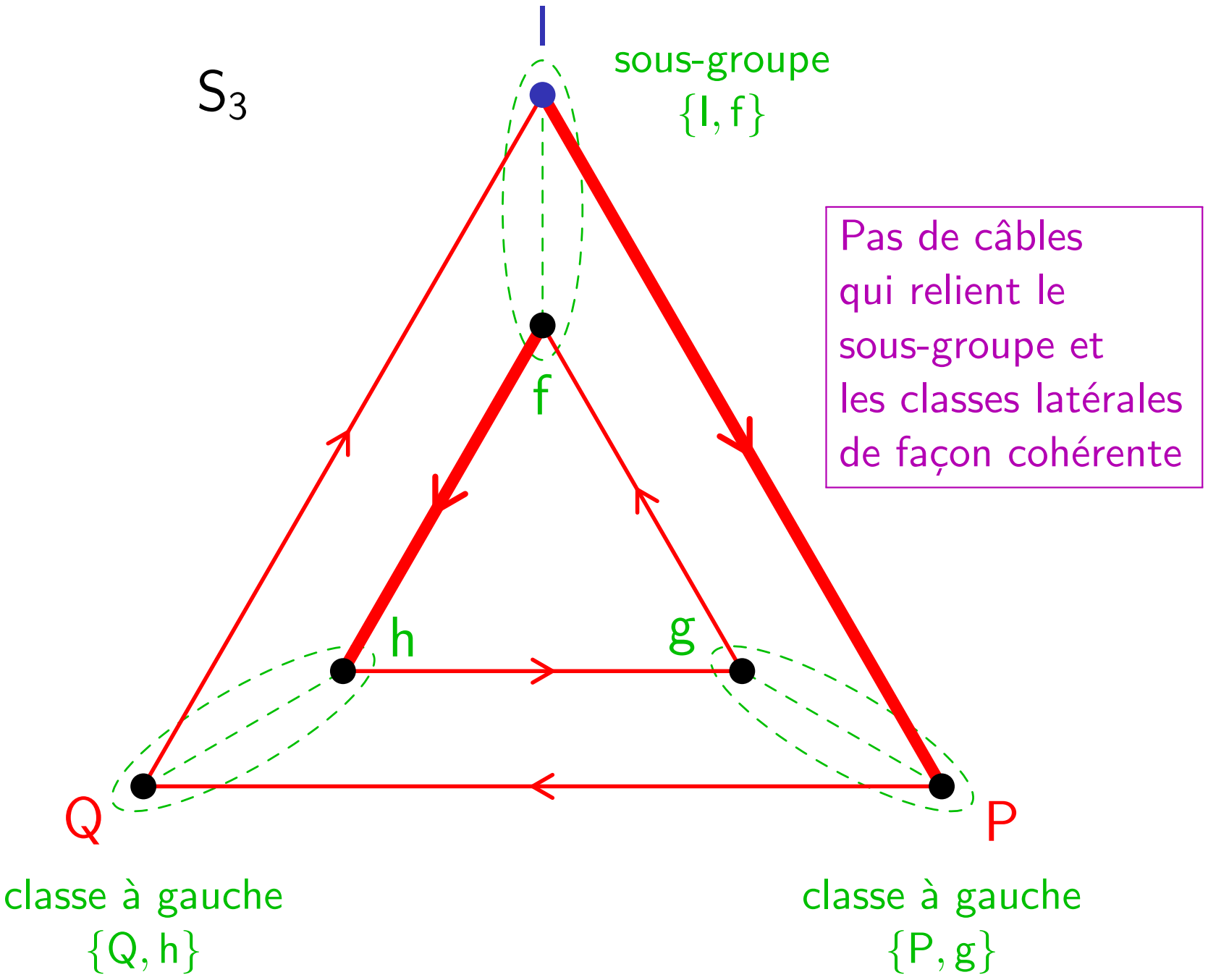

S_3
$S_3/\mathbb{Z}_3$
$\mathbb{Z}_2$
I
Q
P
$\mathbb{Z}_3 = \{I, P, Q\}$
sous-
groupe
le
câble
classe
latérale
f
h
g
$\{f, g, h\}$

sous-groupe

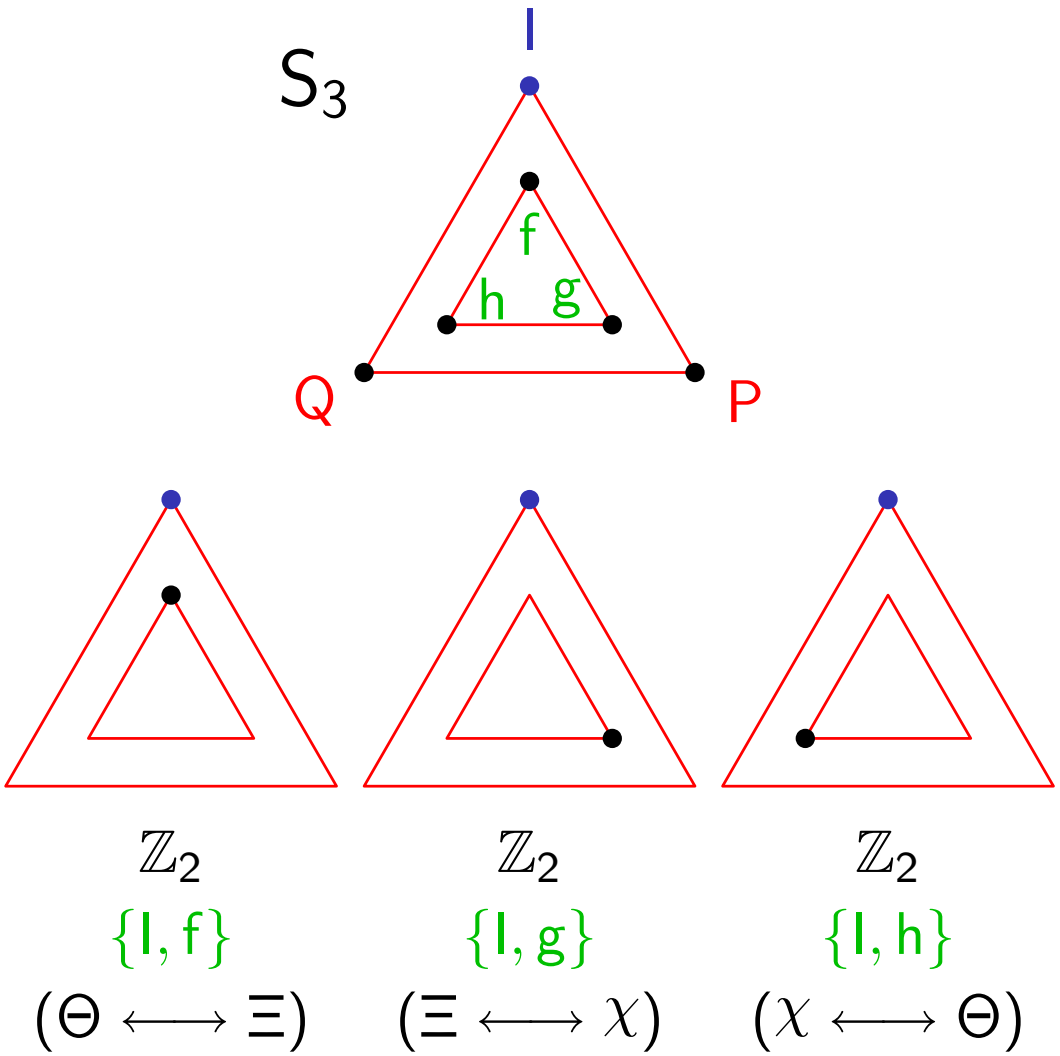
classes à gauche du sous-groupe

	I	f	P	g	Q	h
I	I	f	P	g	Q	h
f	f	I	h	Q	g	P
P	P	g	Q	h	I	f
g	g	P	f	I	h	Q
Q	Q	h	I	f	P	g
h	h	Q	g	P	f	I

Le groupe quotient $S/\{I, f\}$ n'existe pas !

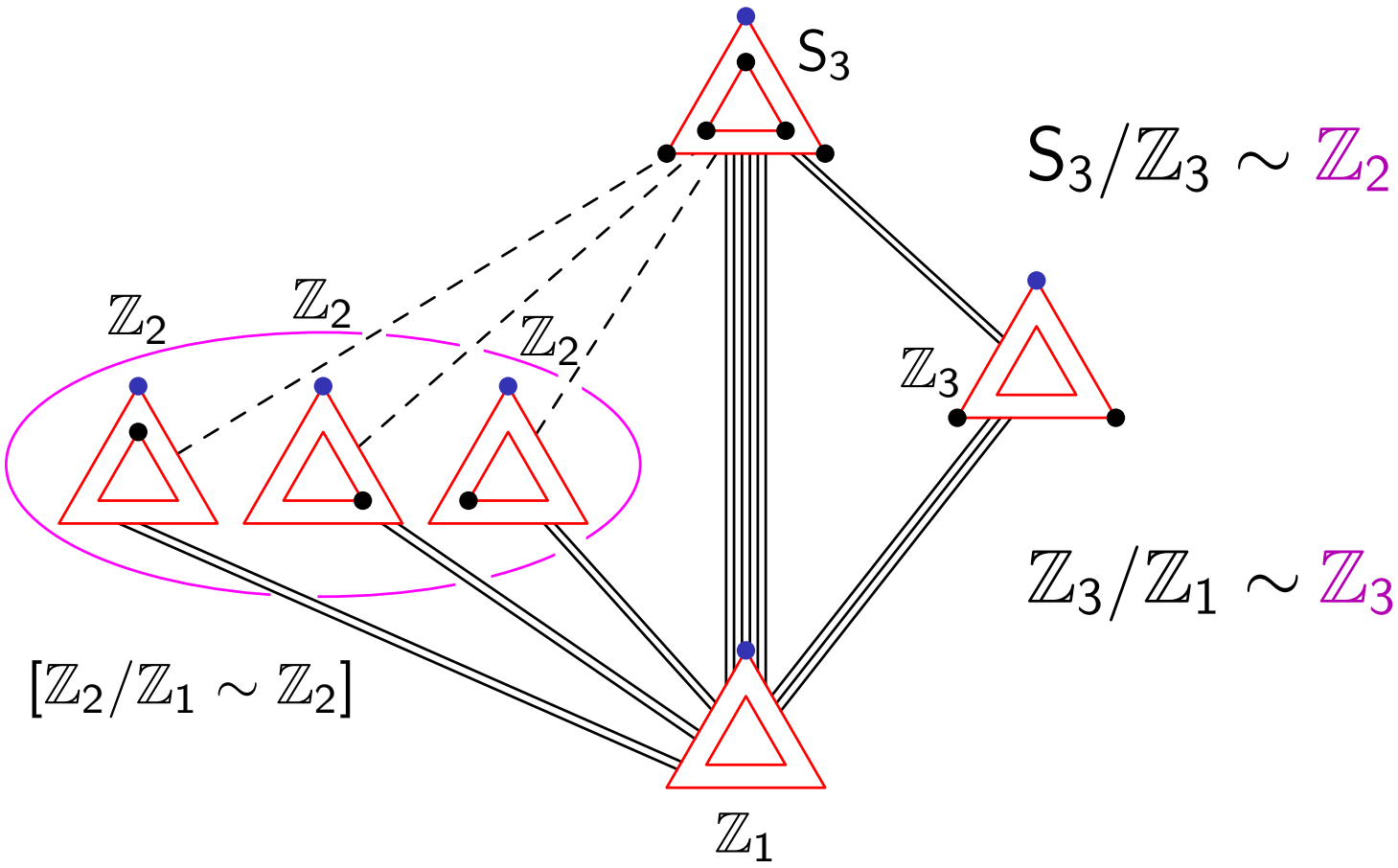

S_3
I
sous-groupe
$\{I, f\}$
Pas de câbles
qui relient le
sous-groupe et
les classes latérales
de façon cohérente
f
h
g
Q
P
classe à gauche
$\{Q, h\}$
classe à gauche
$\{P, g\}$

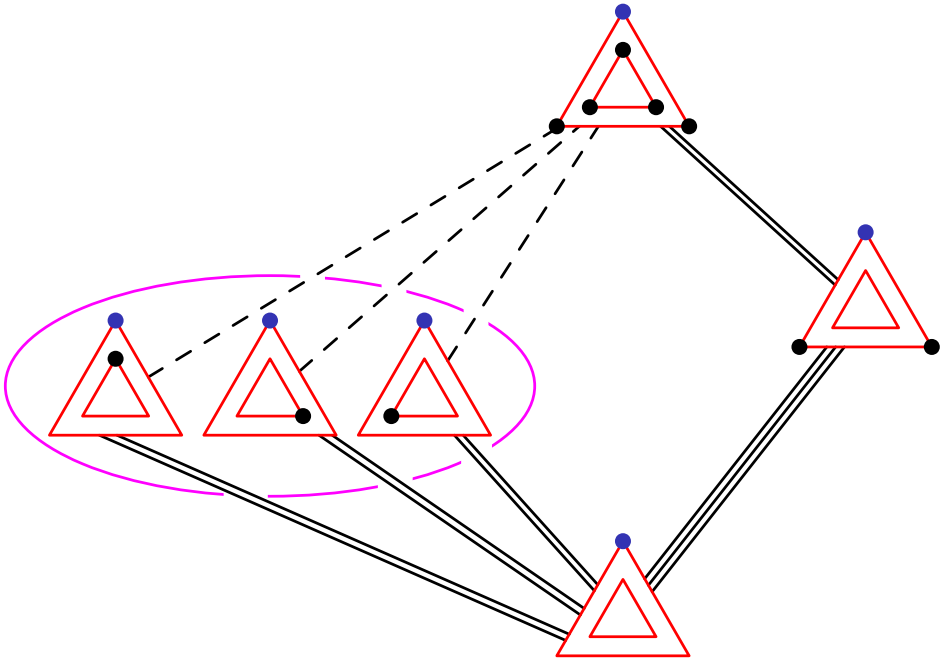
Vers le treillis de sous-groupes de S_3

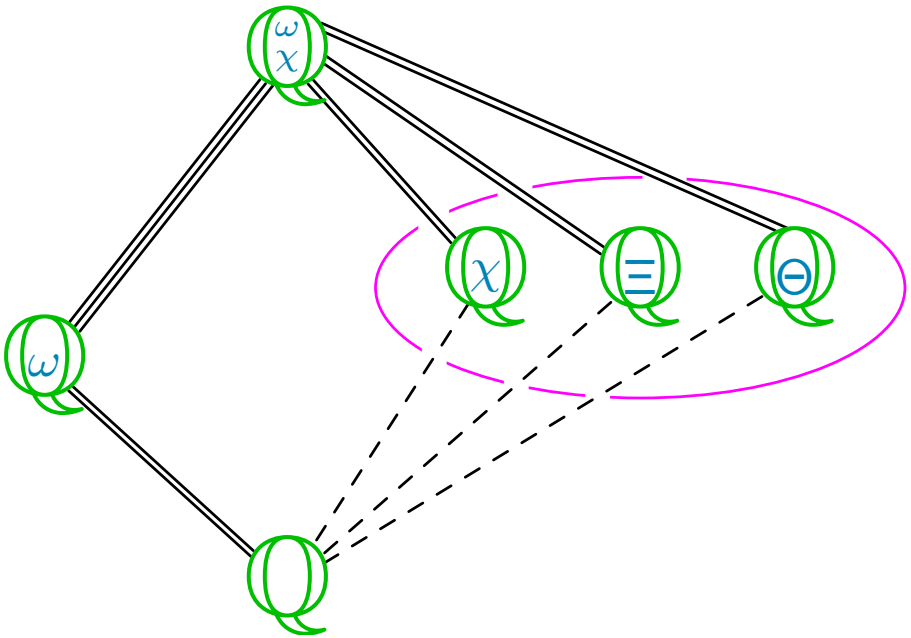


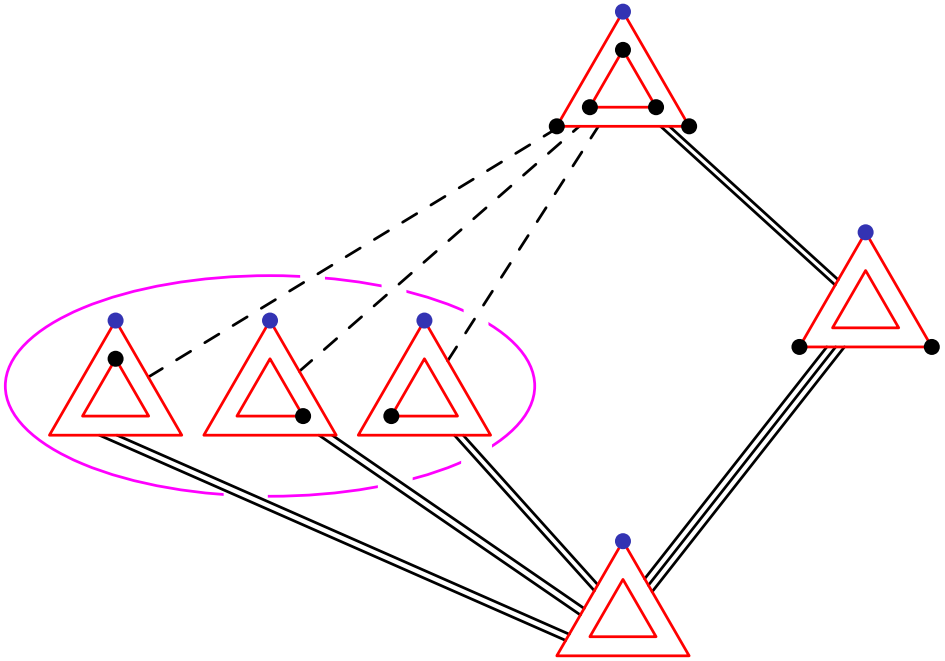
Trois sous-groupes *non* distingués d'ordre 2, tous isomorphes (« sous-groupes conjugués »)

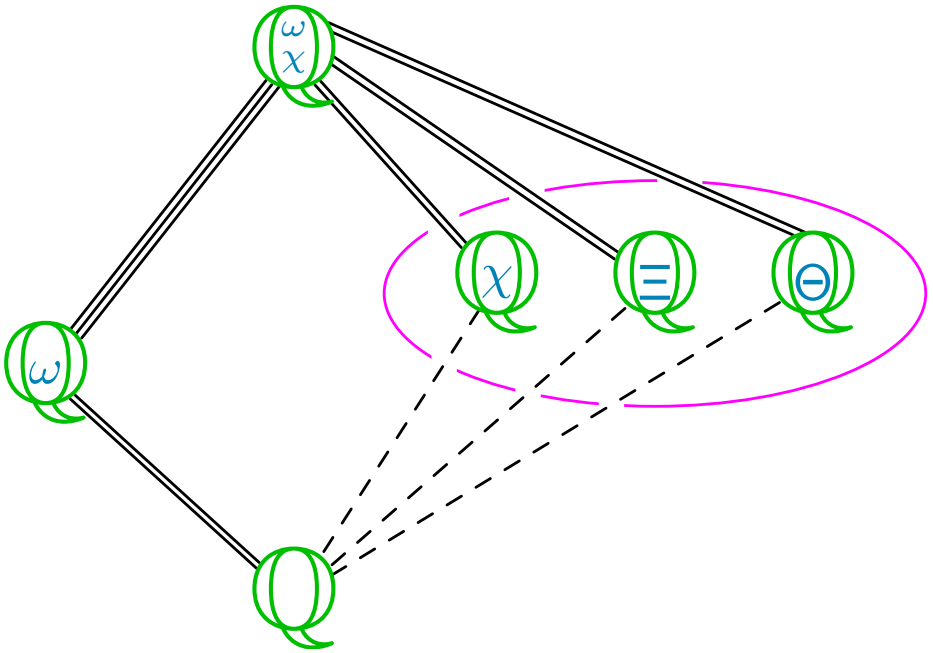
Le treillis de sous-groupes de S_3

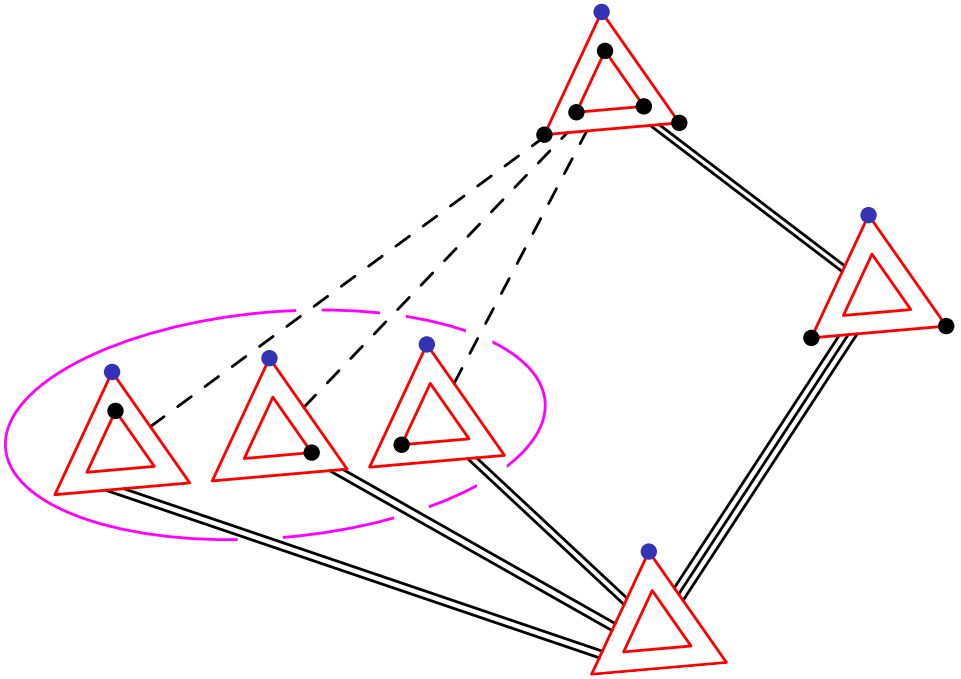


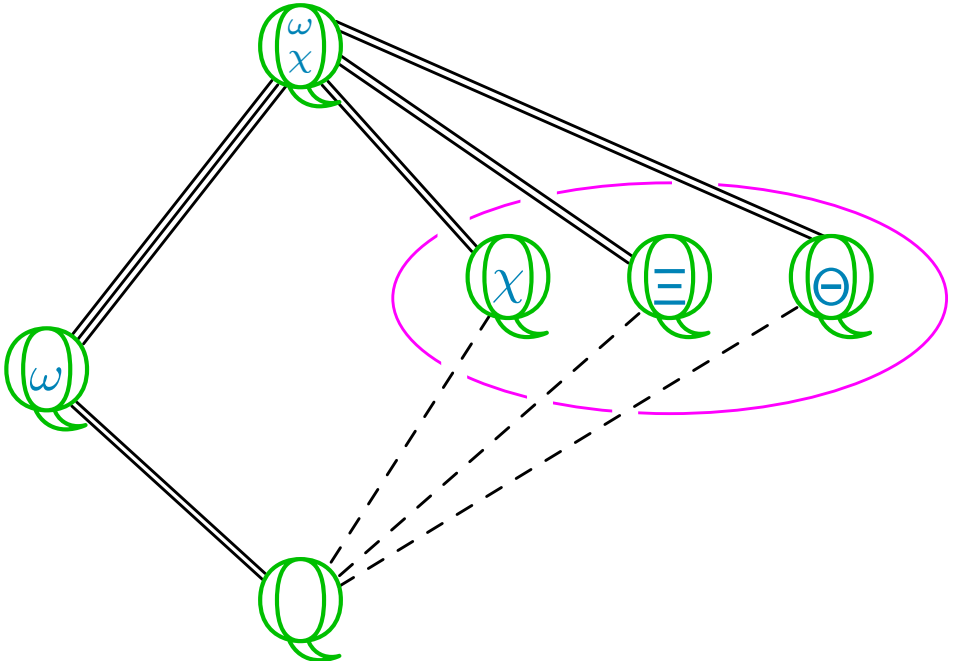


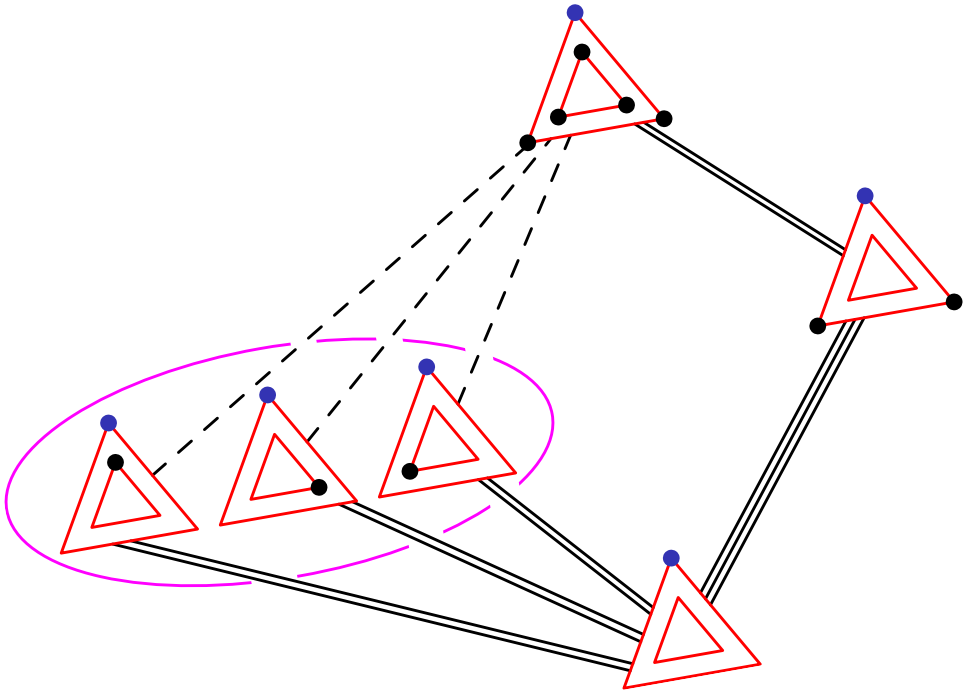

ω
χ
χ
≡
Θ
ω

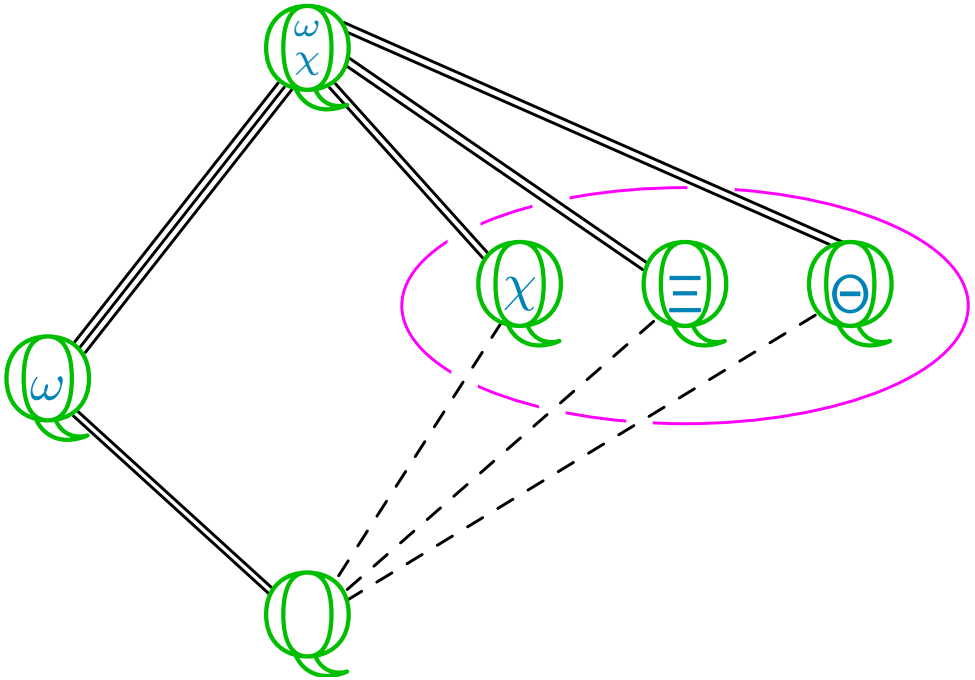


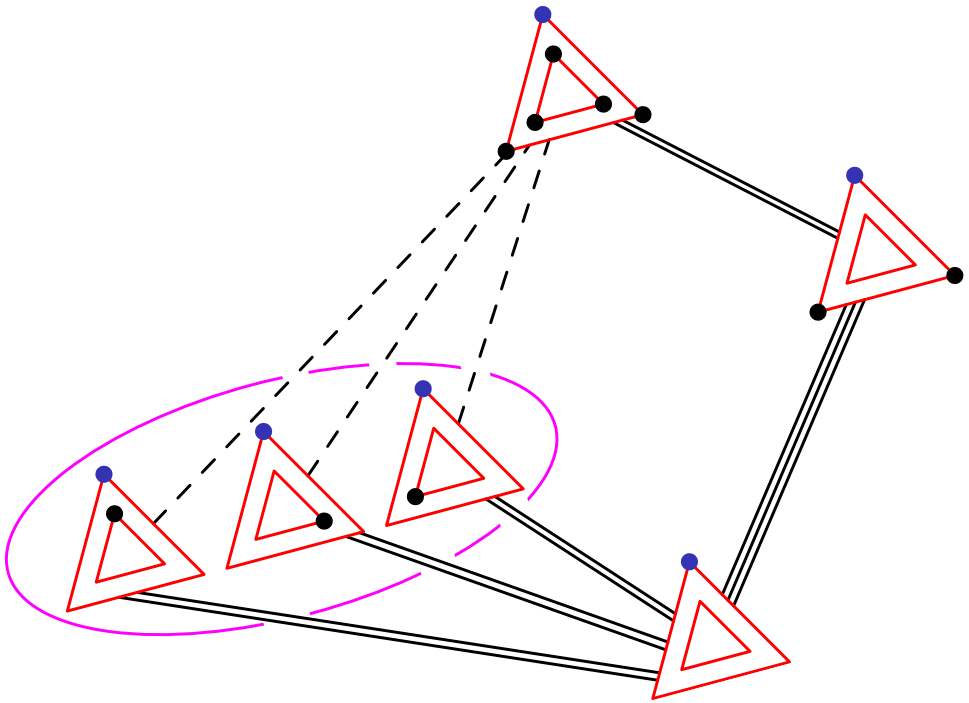

ω
χ
ω
χ
≡
⊖

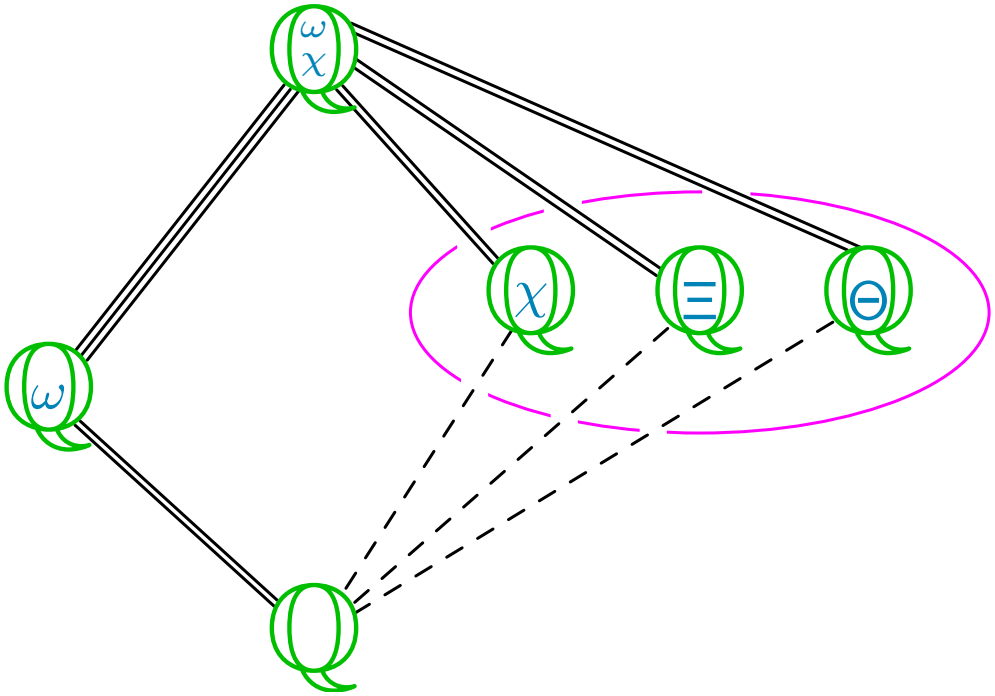


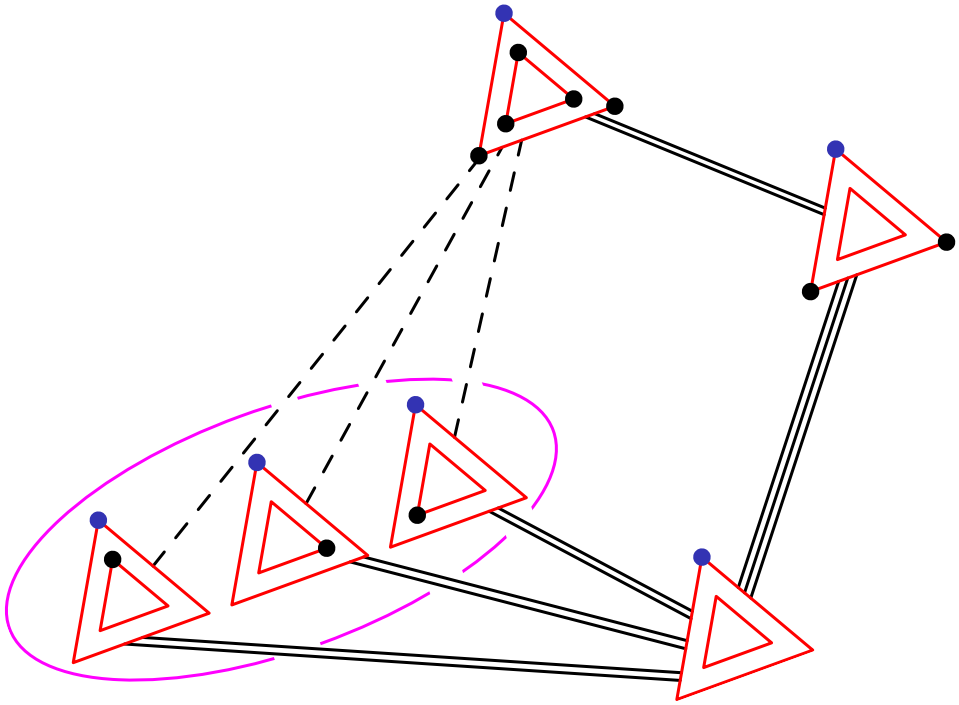

ω
χ
ω
χ
≡
⊖

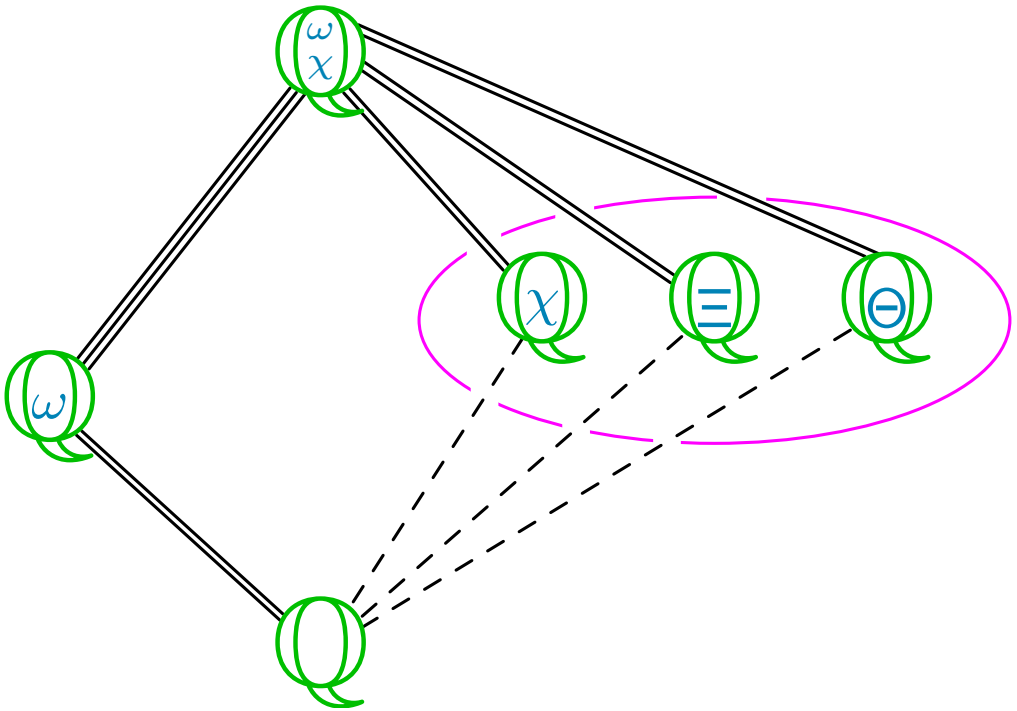


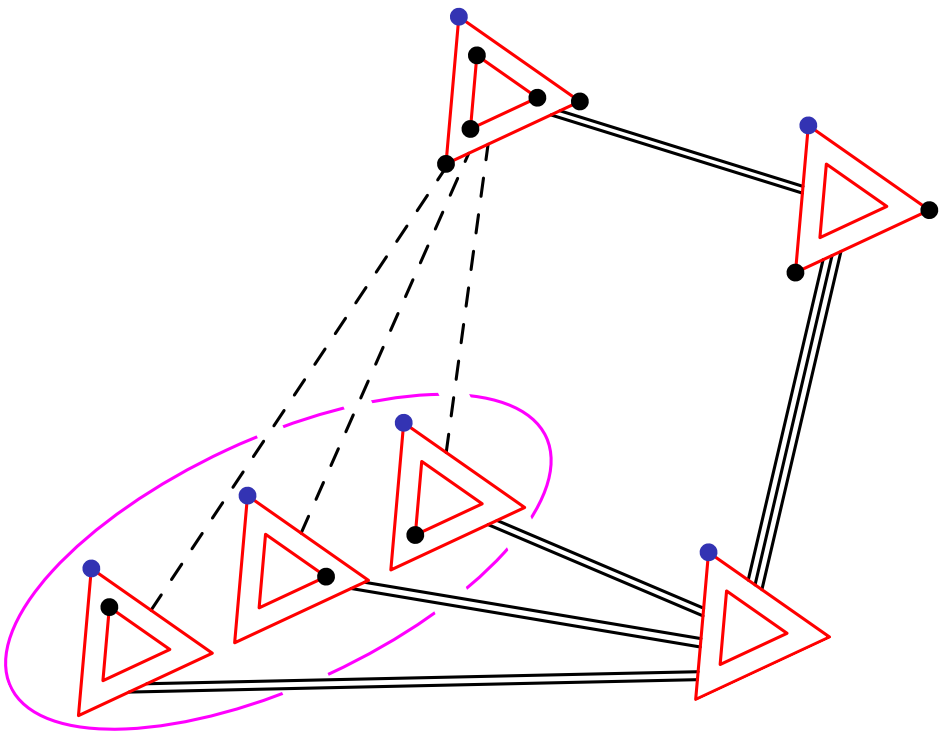

ω
χ
χ
=
⊖
ω

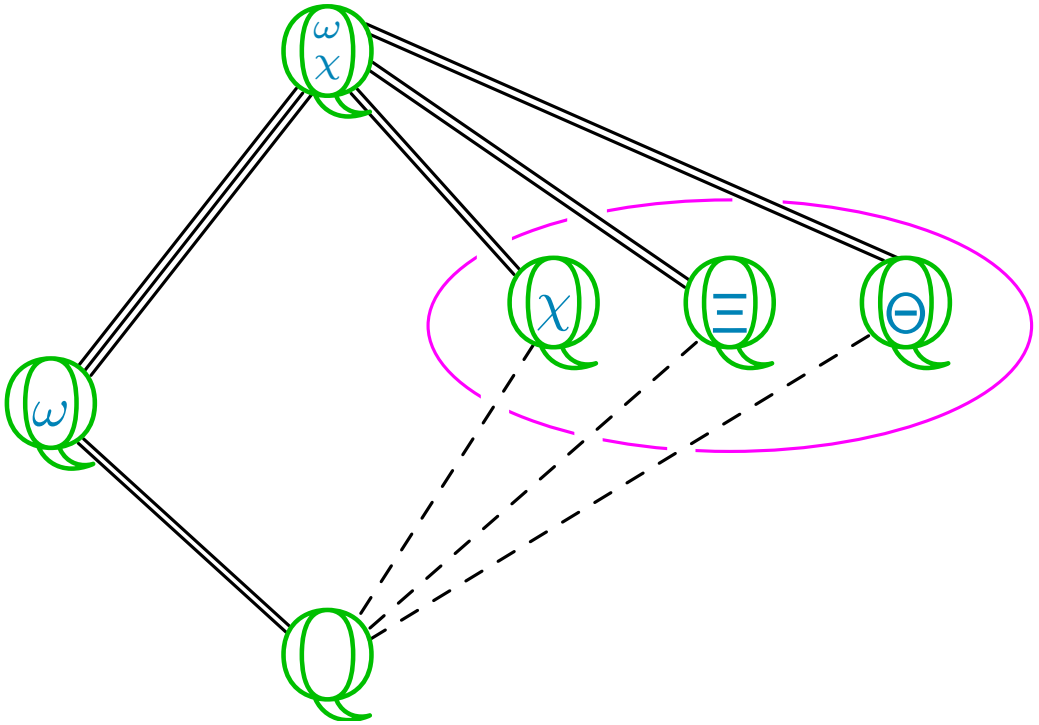


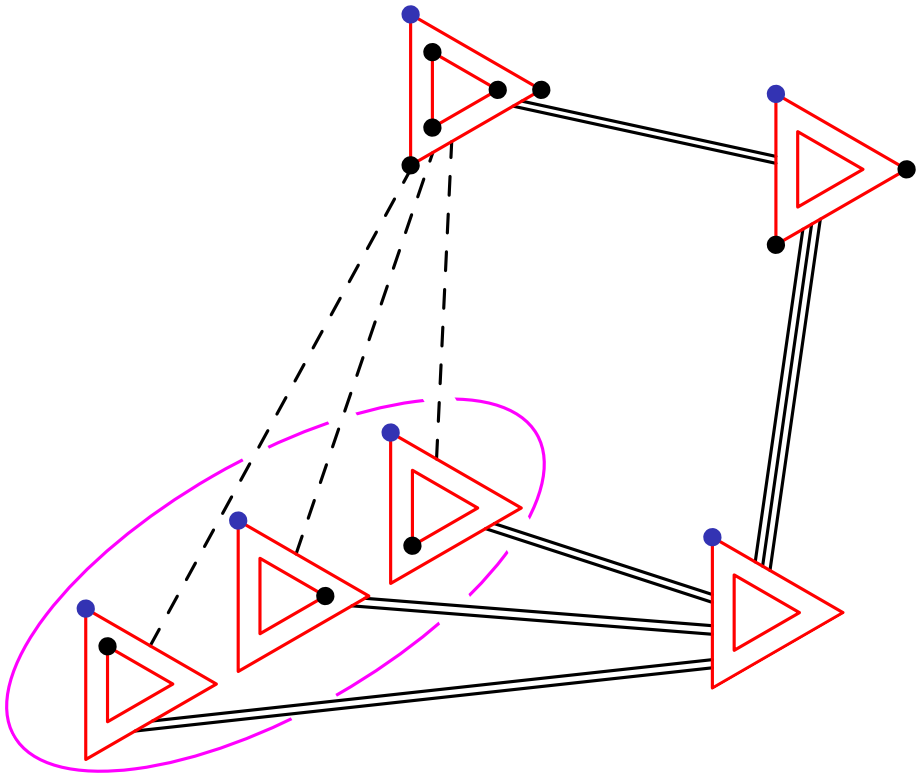

ω
χ
ω
χ
≡
⊖

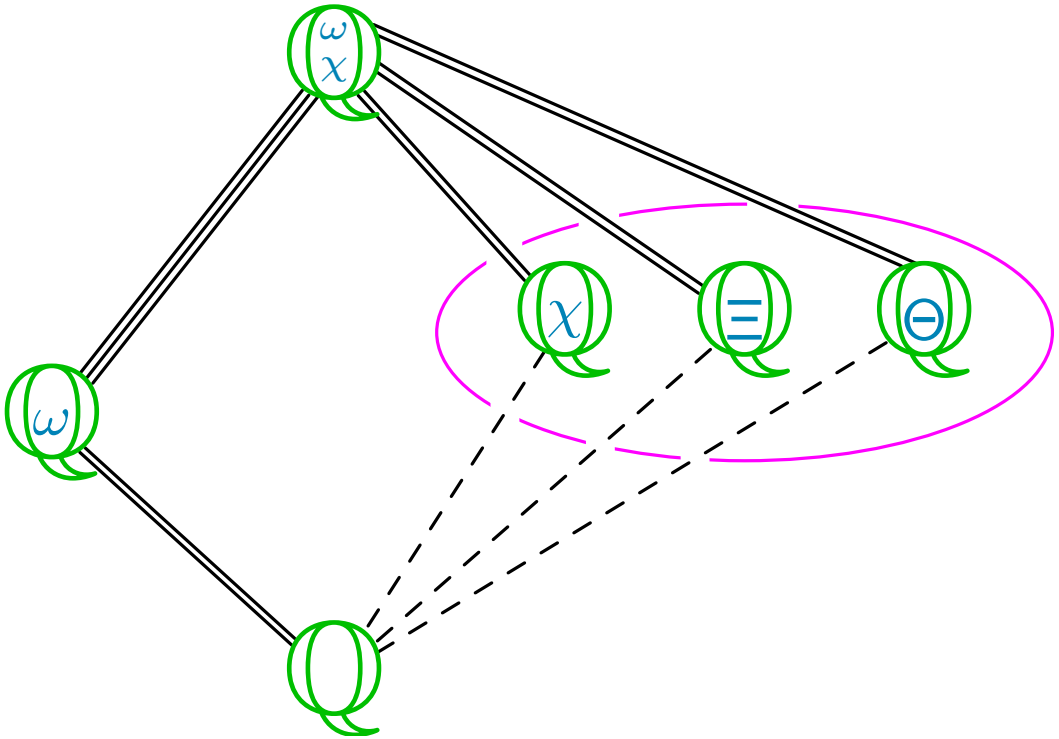


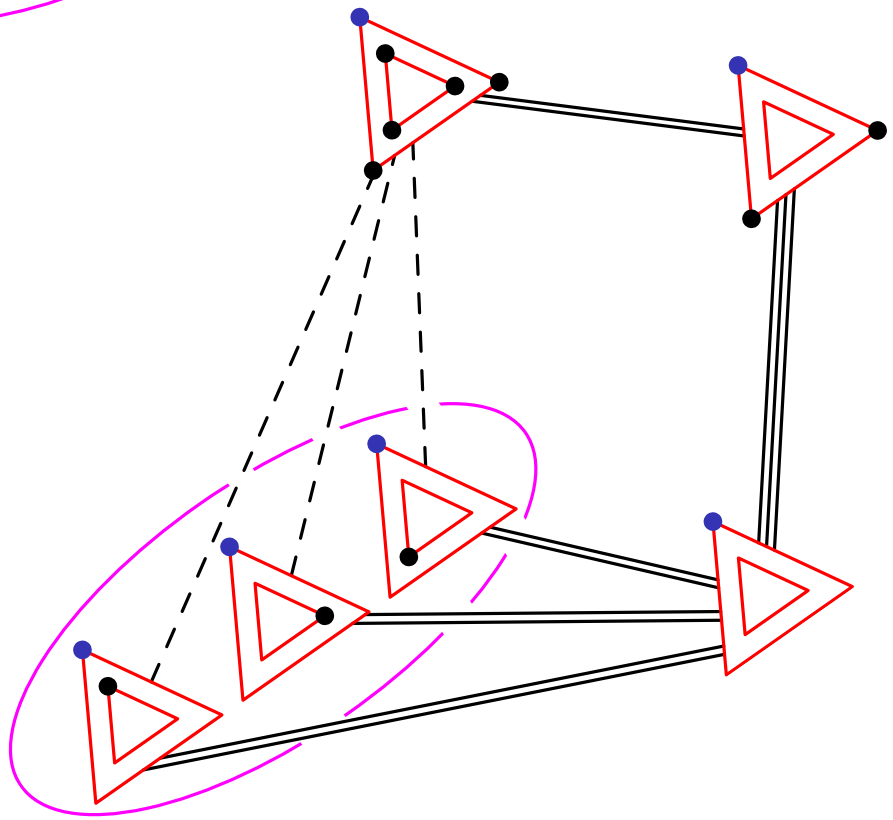

ω
χ
χ
≡
⊖
ω

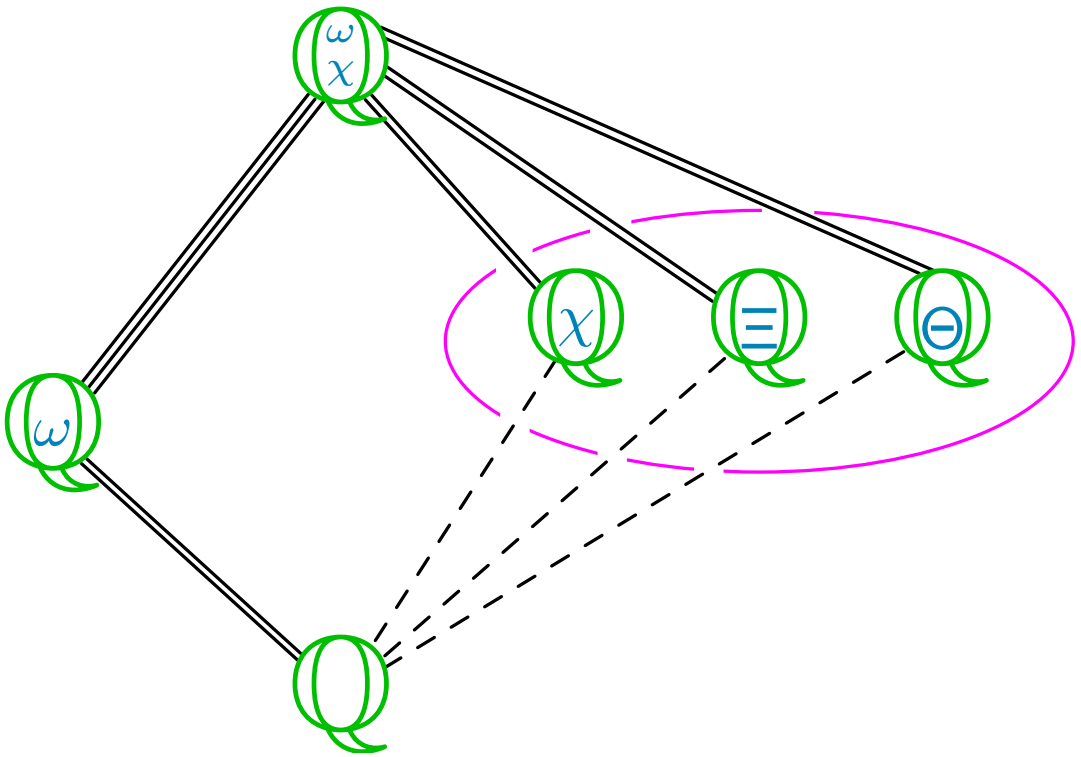


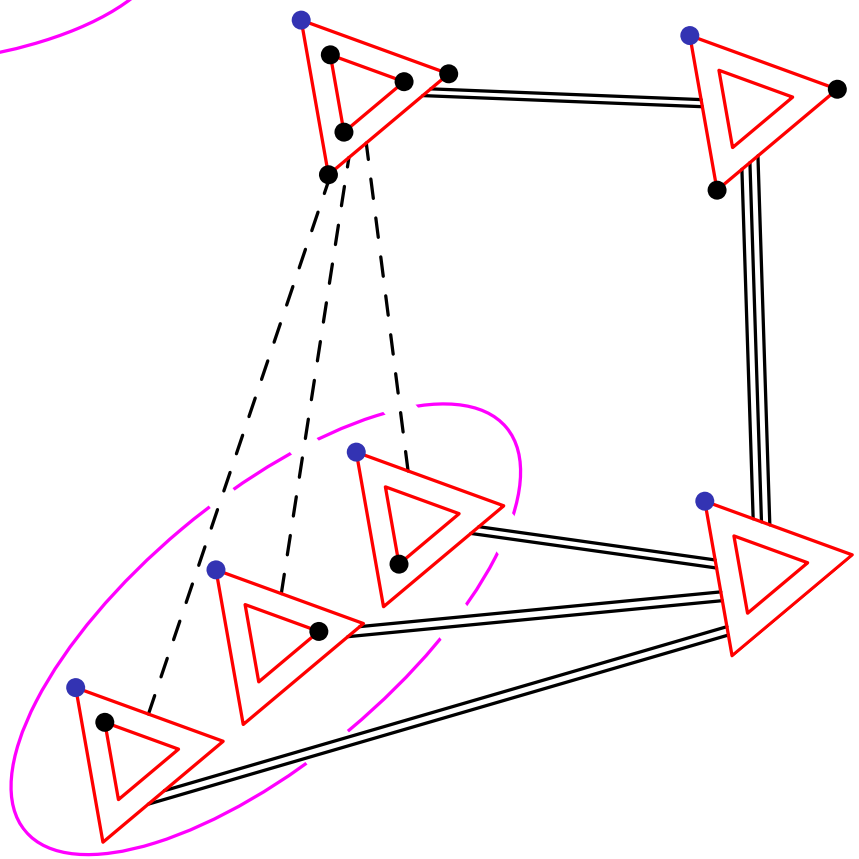

ω
χ
ω
χ
≡
⊖

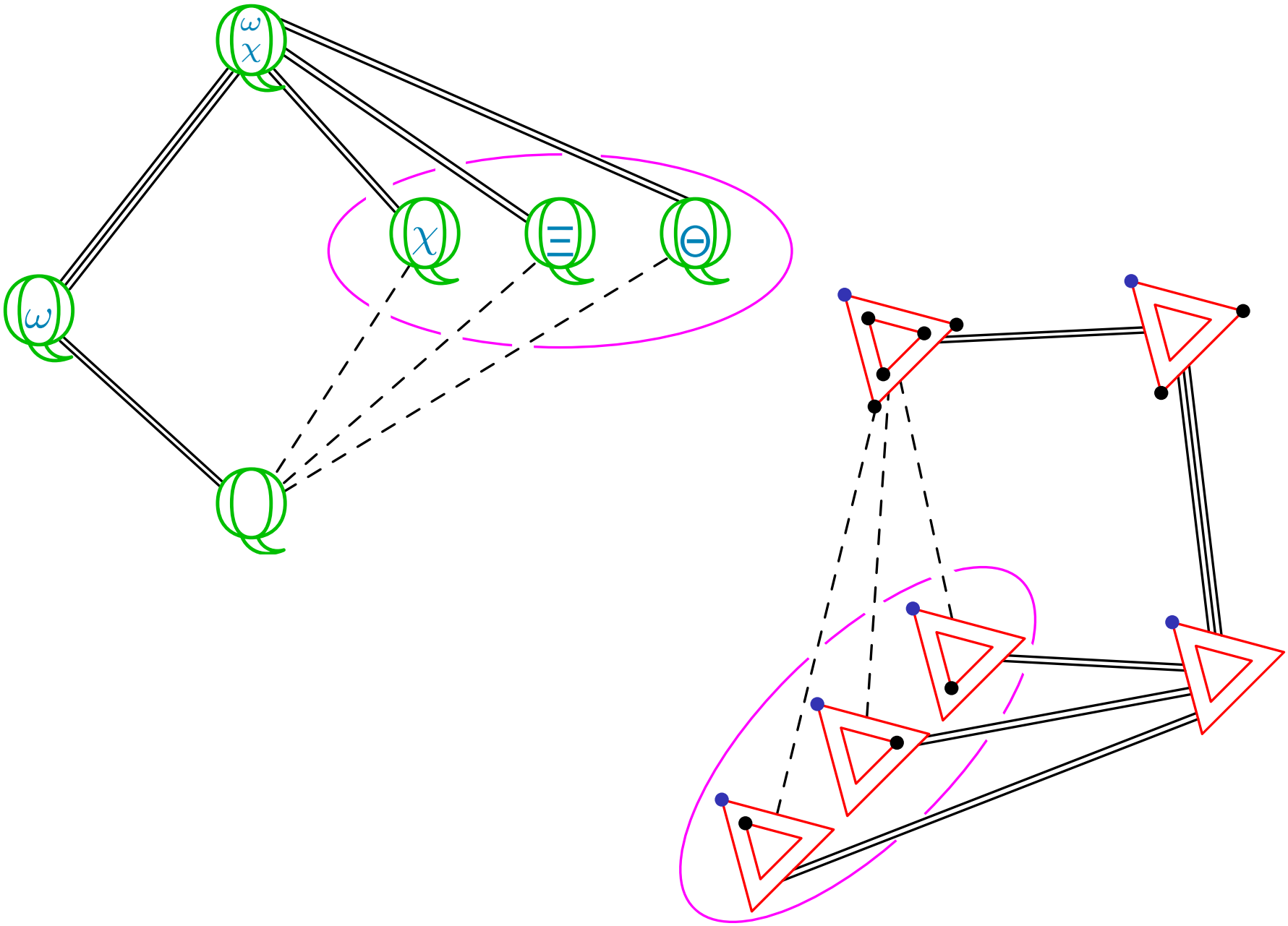


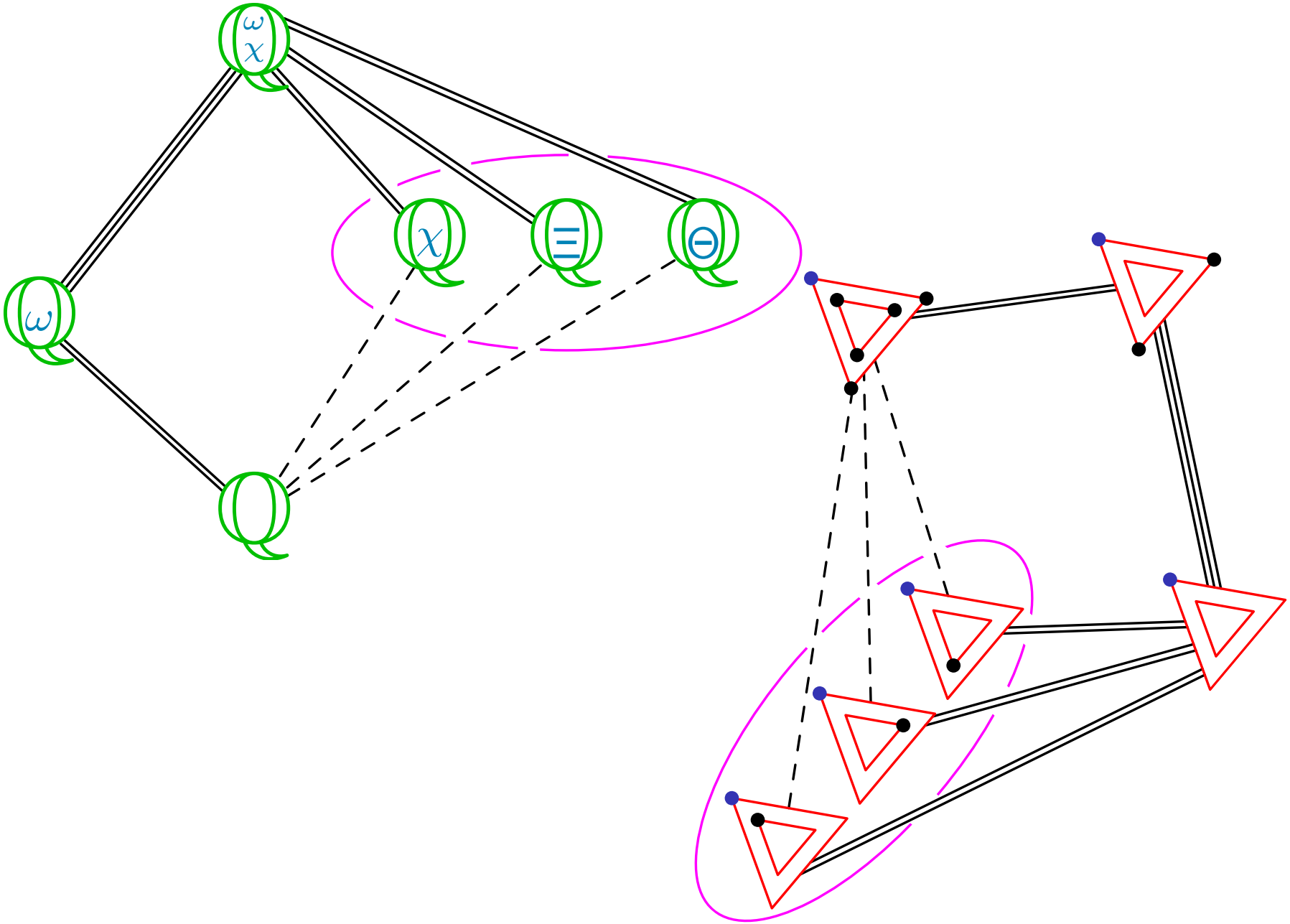

ω
χ
ω
χ
≡
⊖

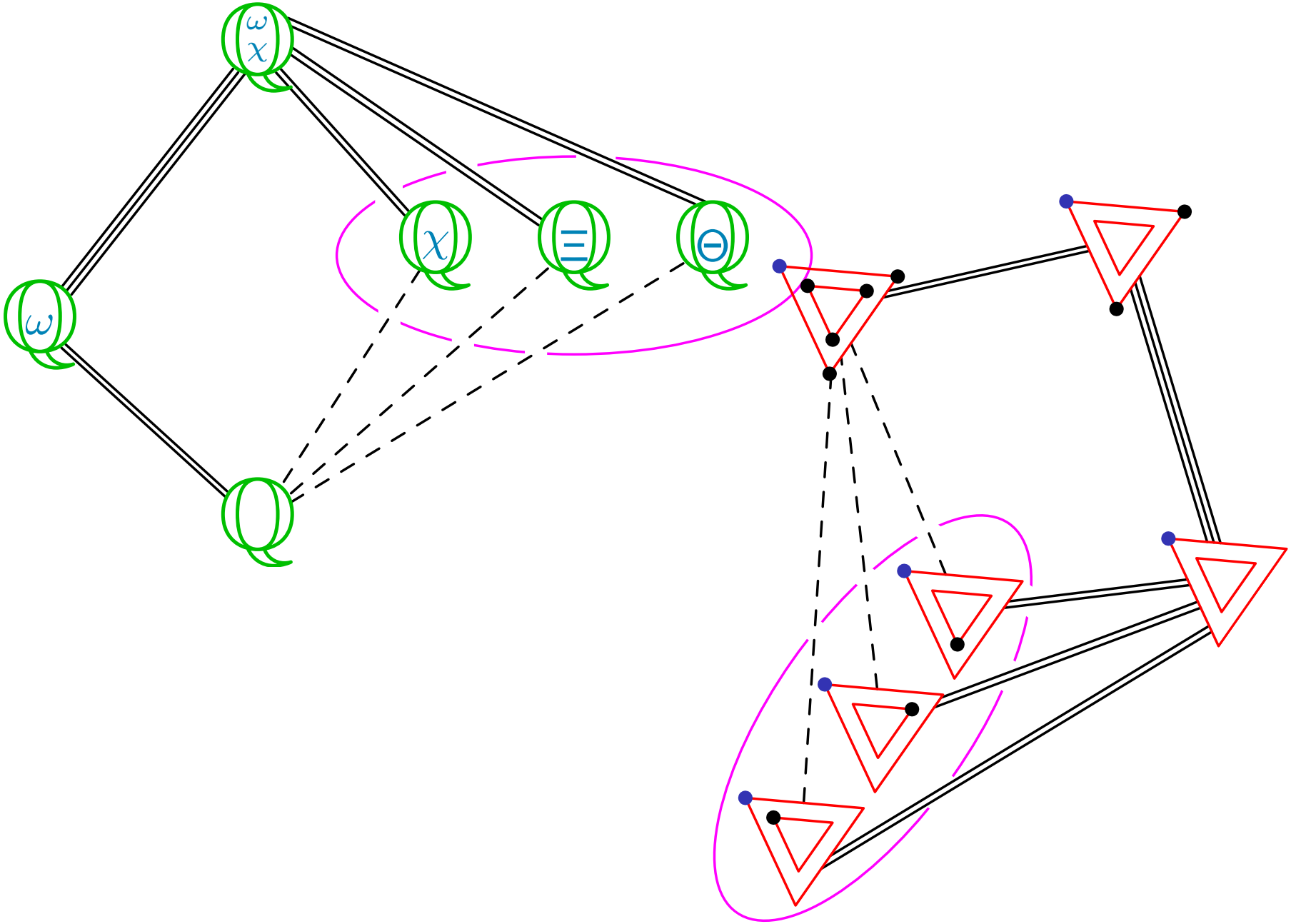


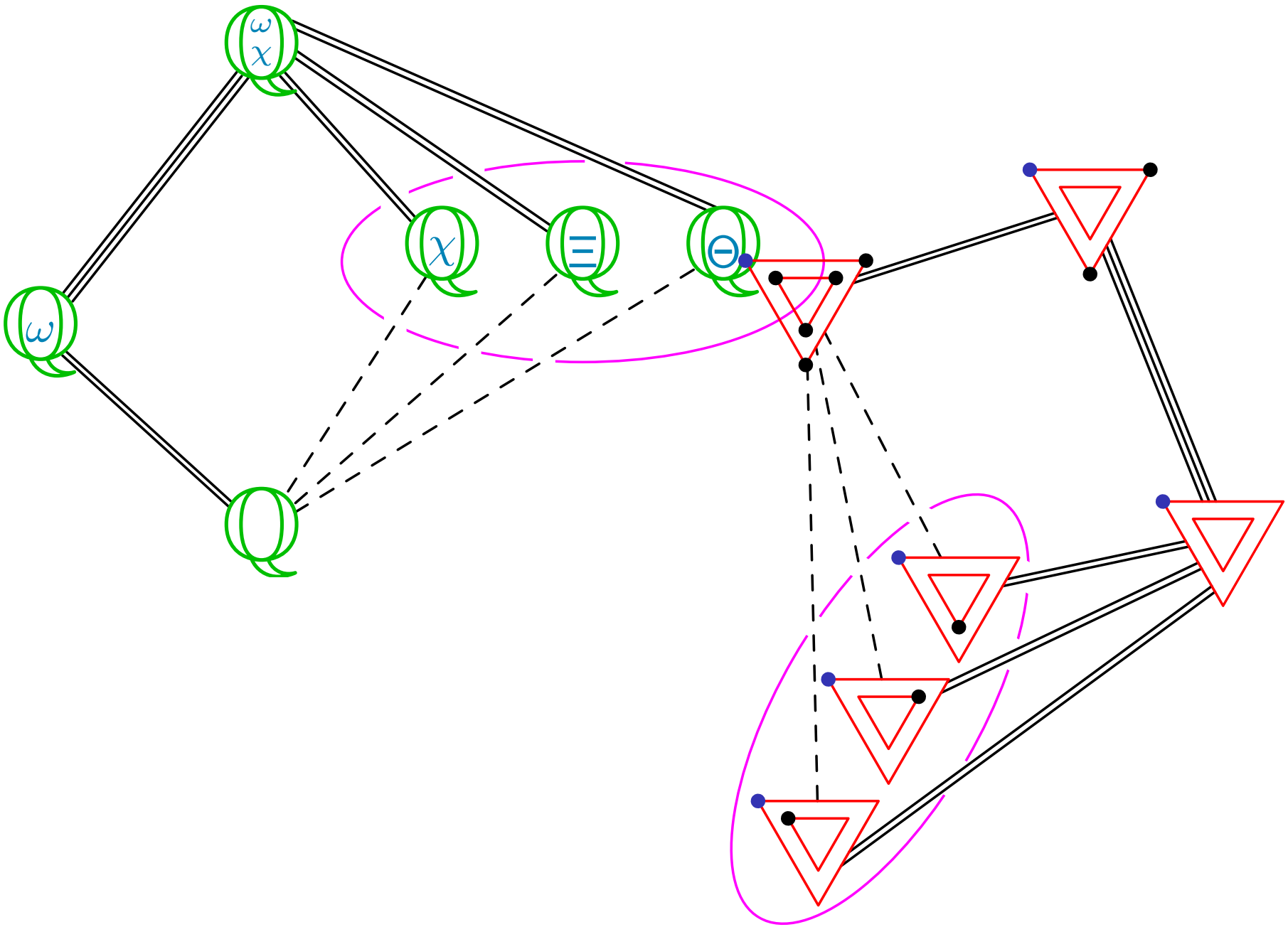

ω
χ
ω
χ
≡
⊖

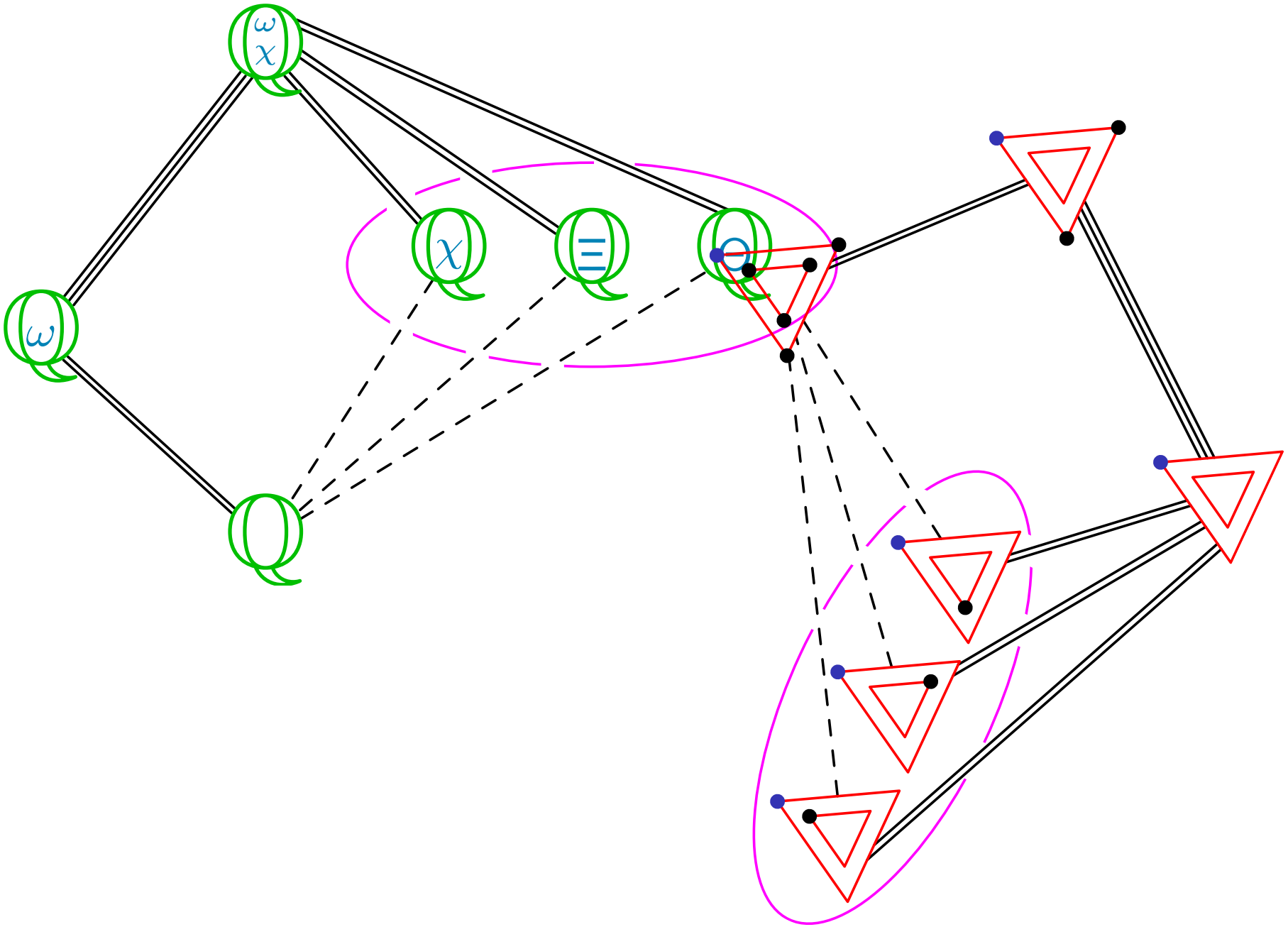


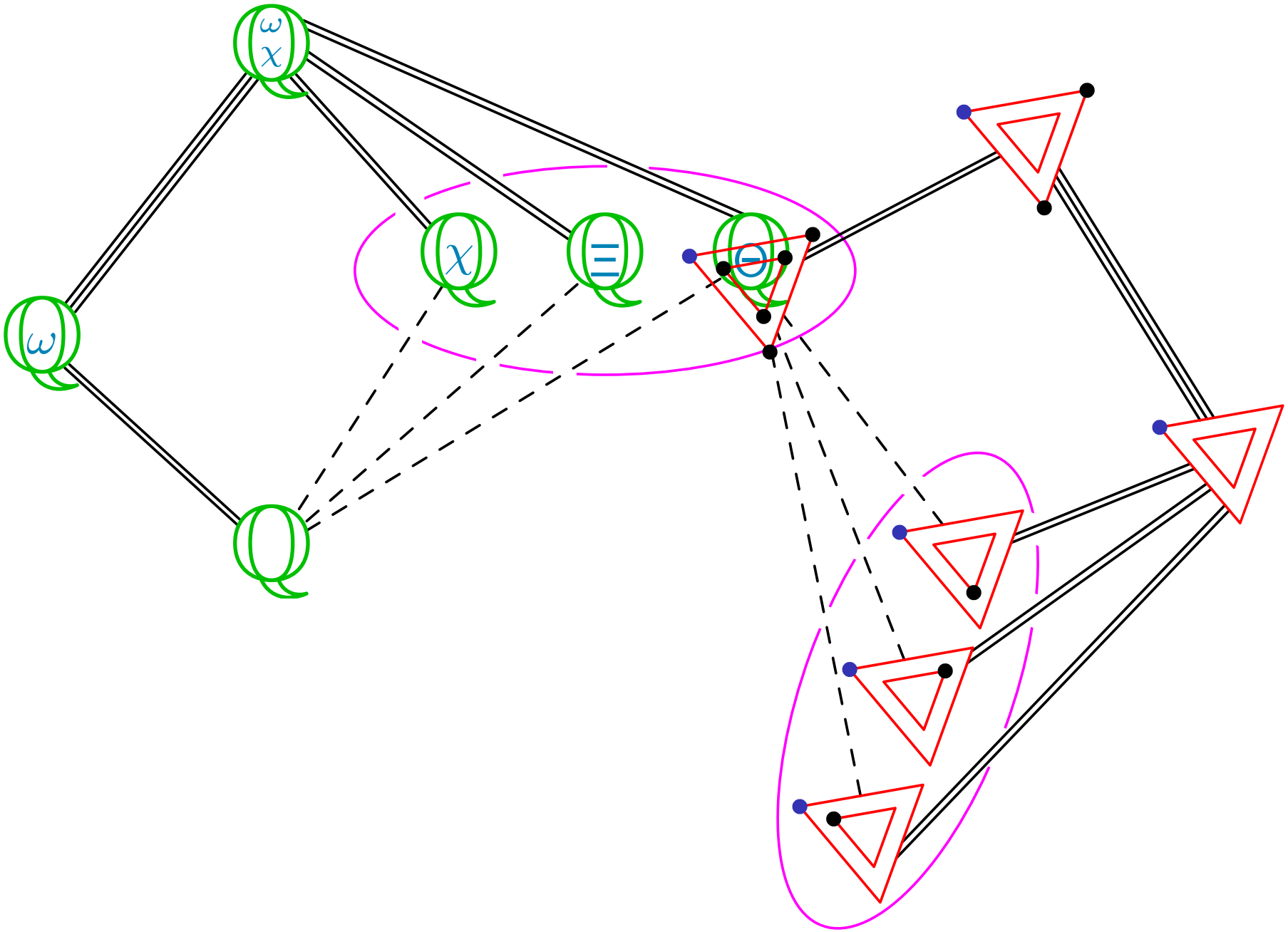

ω
χ
χ
≡
⊖
ω

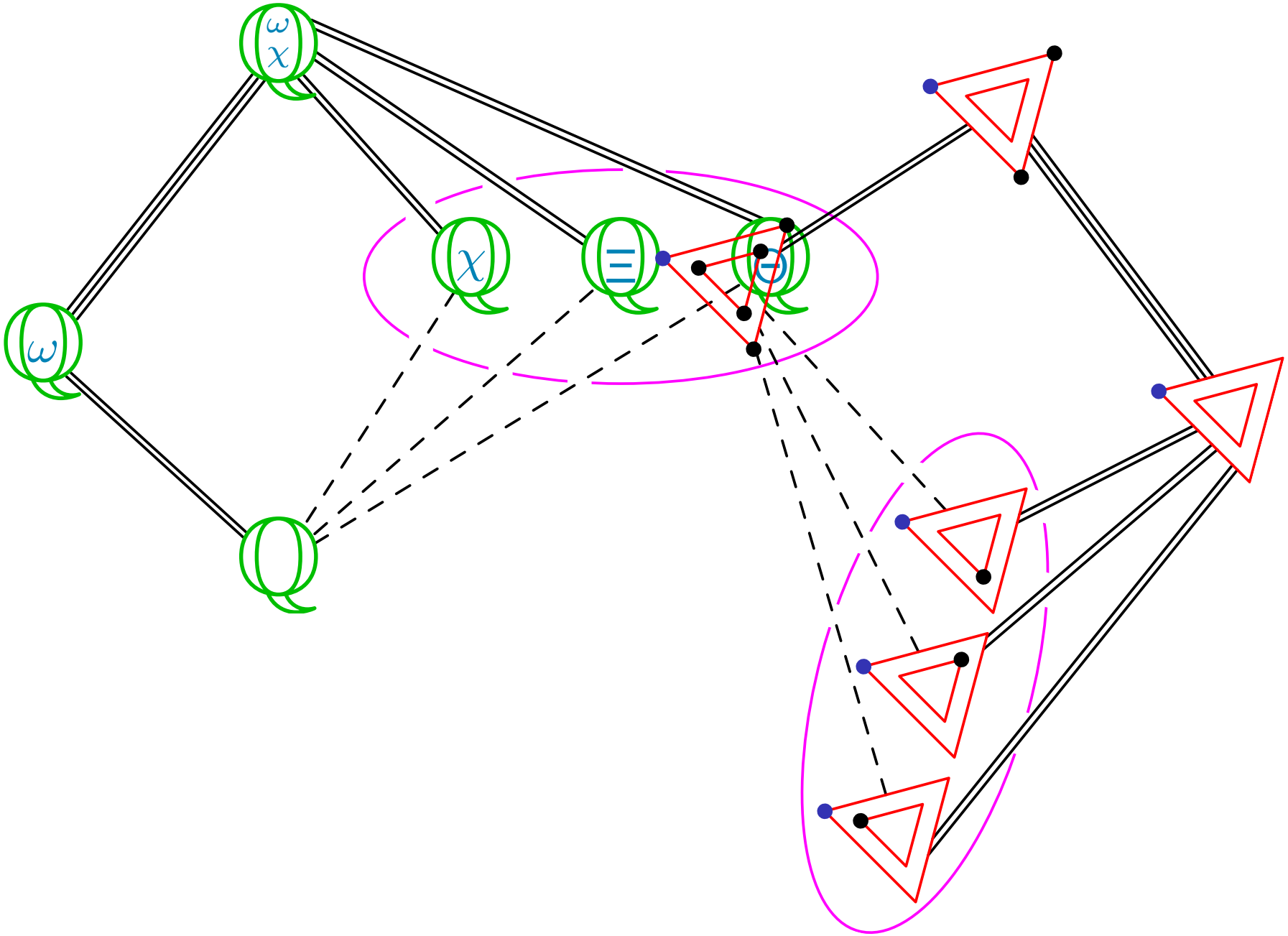

ω
χ
ω
χ
≡
⊖

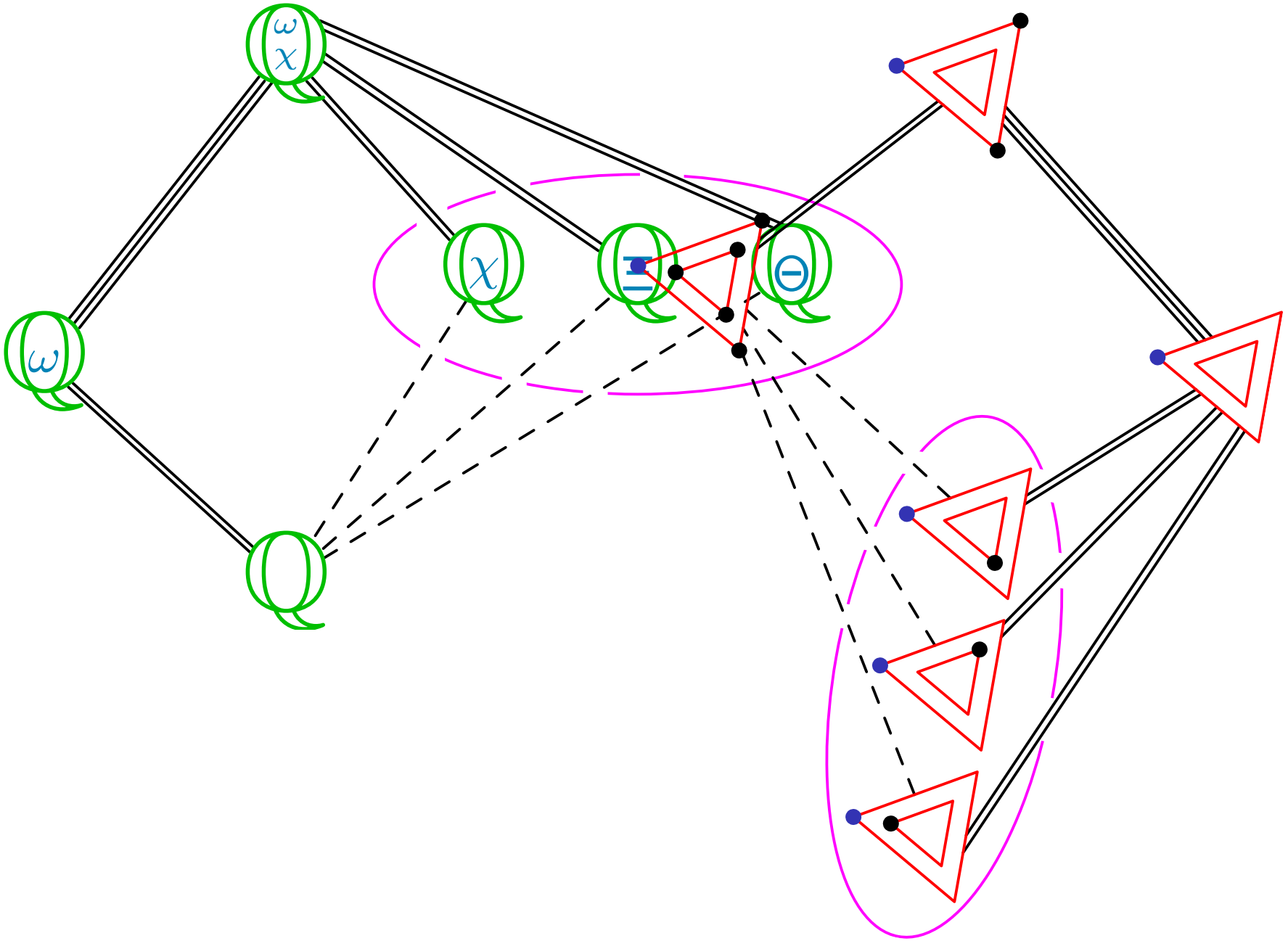

ω
χ
χ
≡
⊖
ω

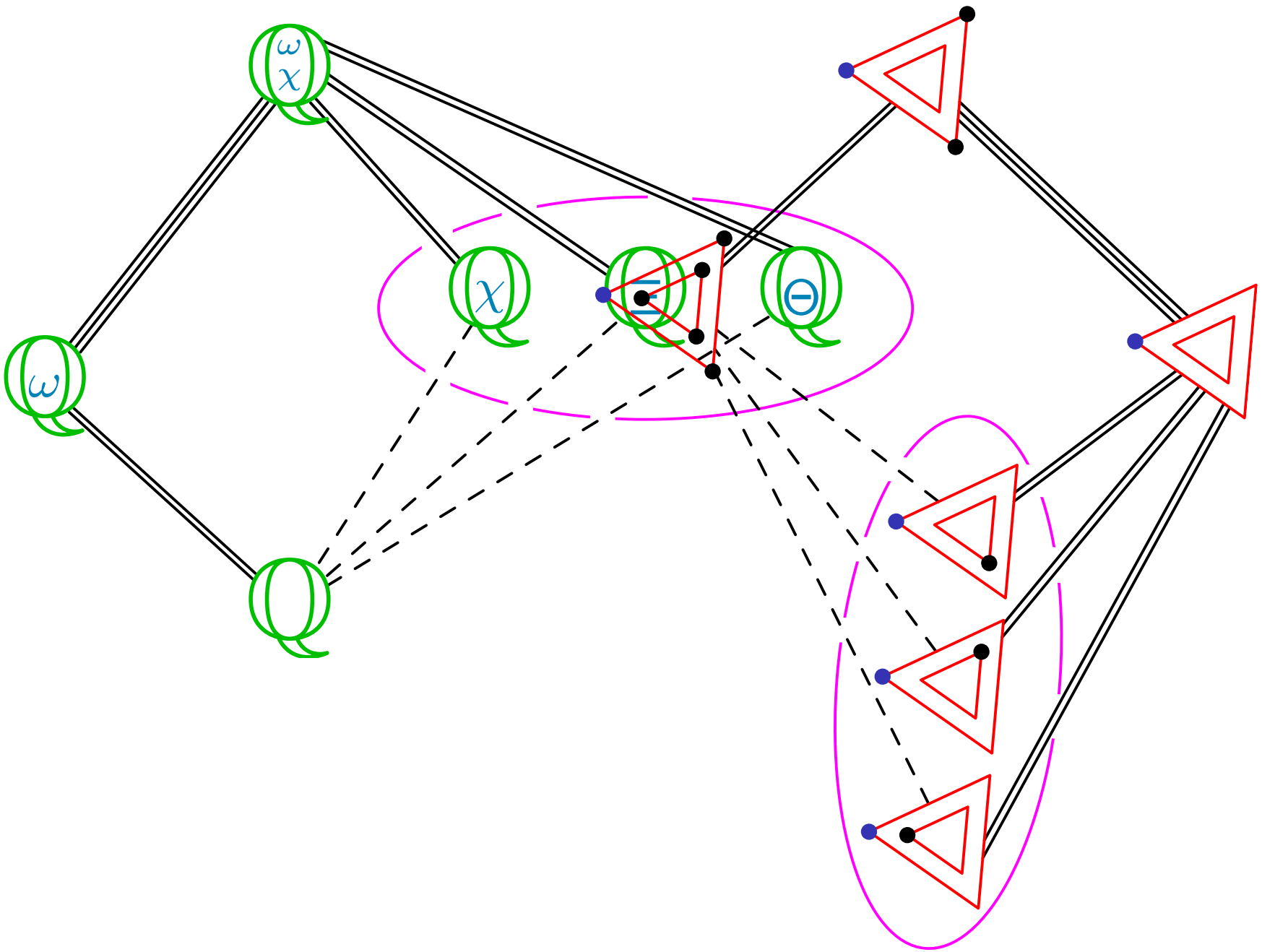

ω
χ
χ
≡
Θ
ω

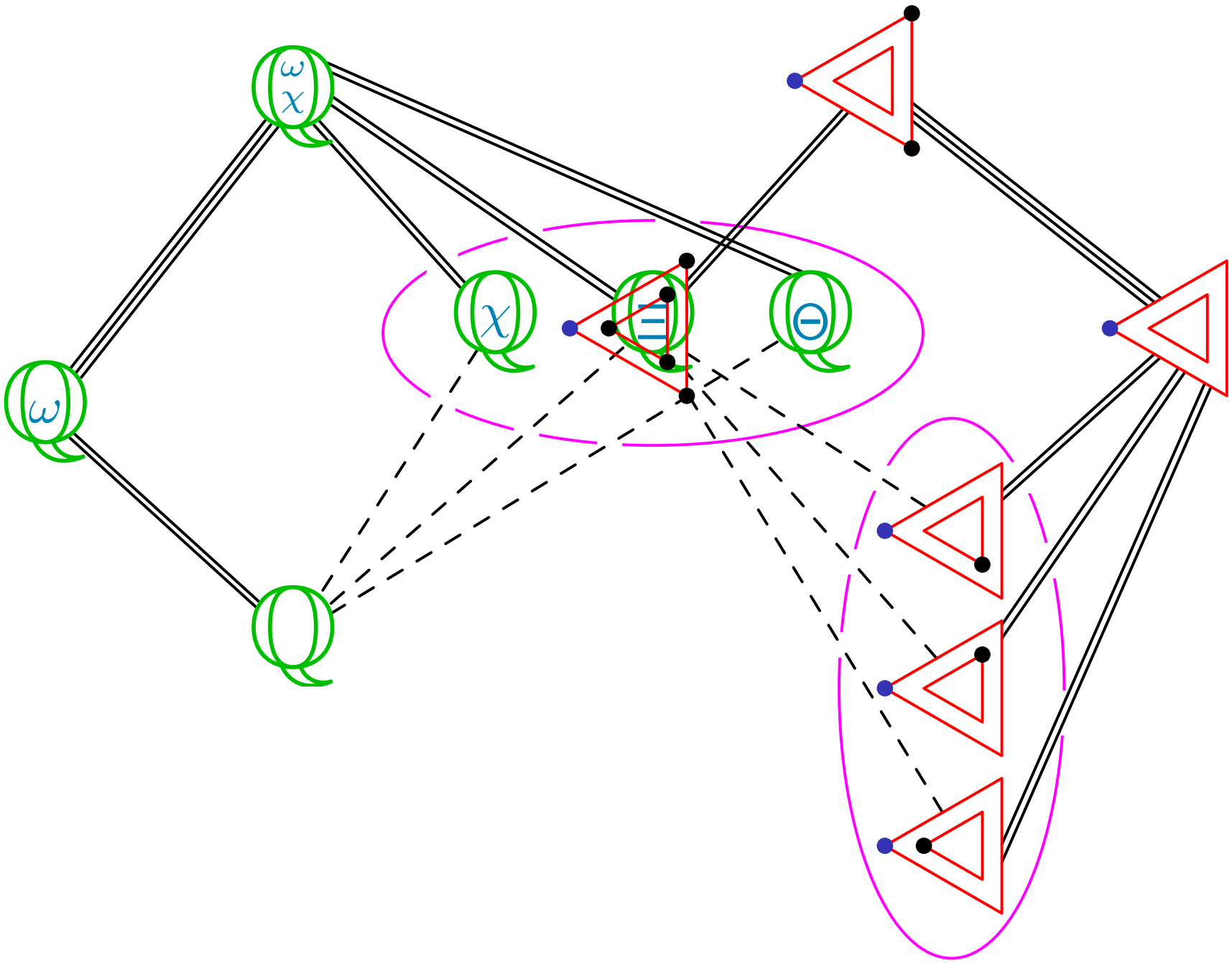

ω
χ
χ
≡
ω

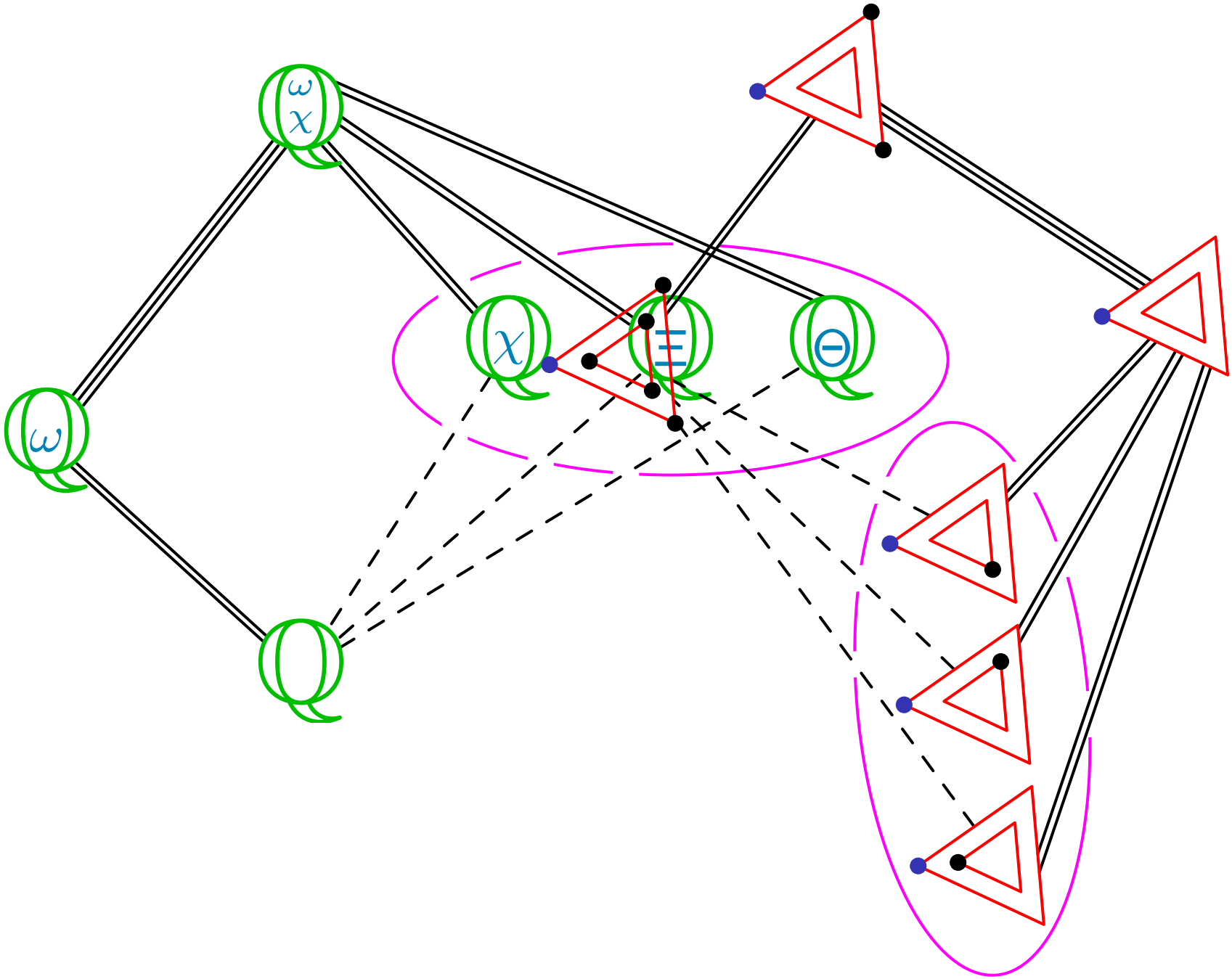

ω
χ
χ
≡
⊖
ω

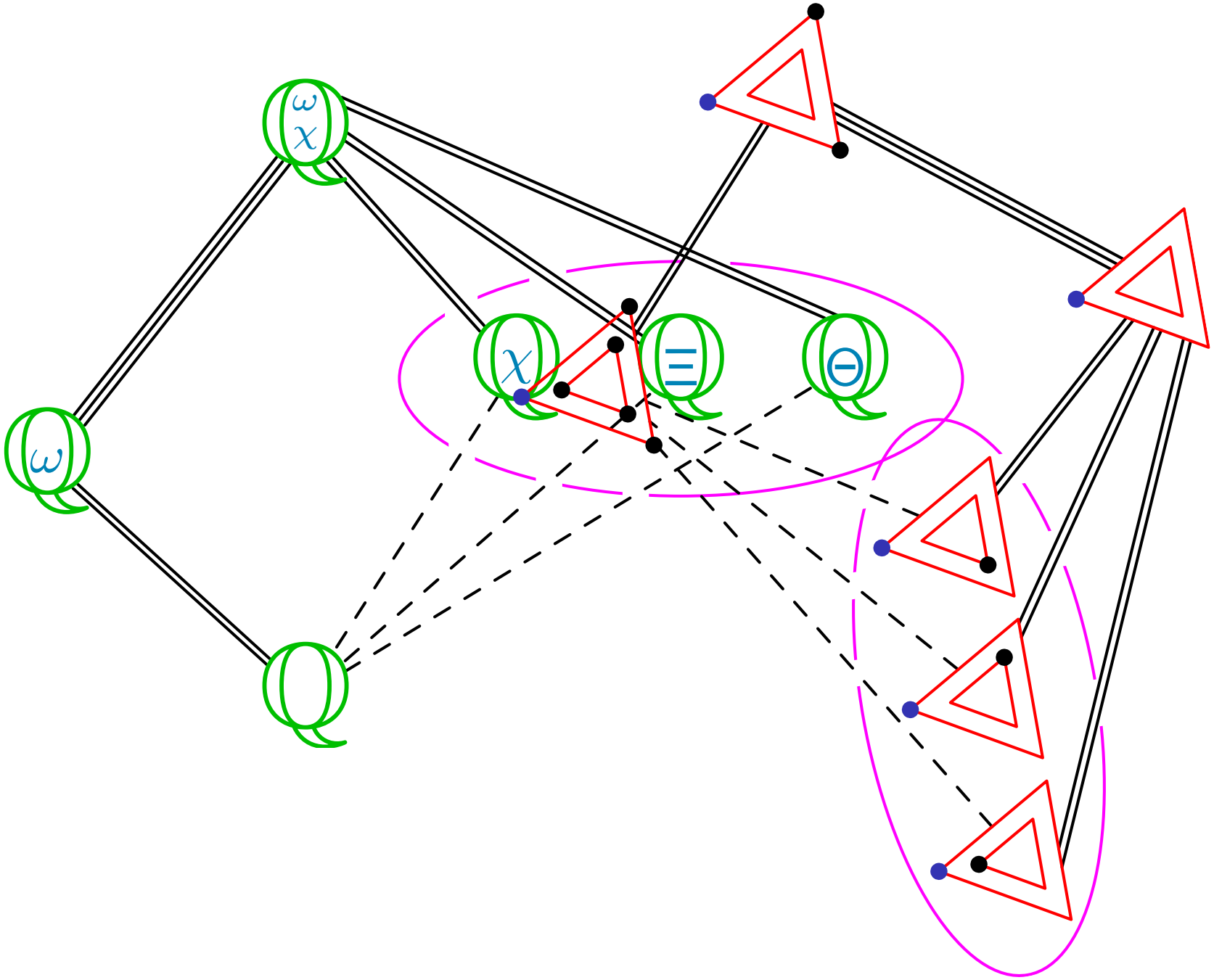

ω
χ
χ
≡
⊖
ω

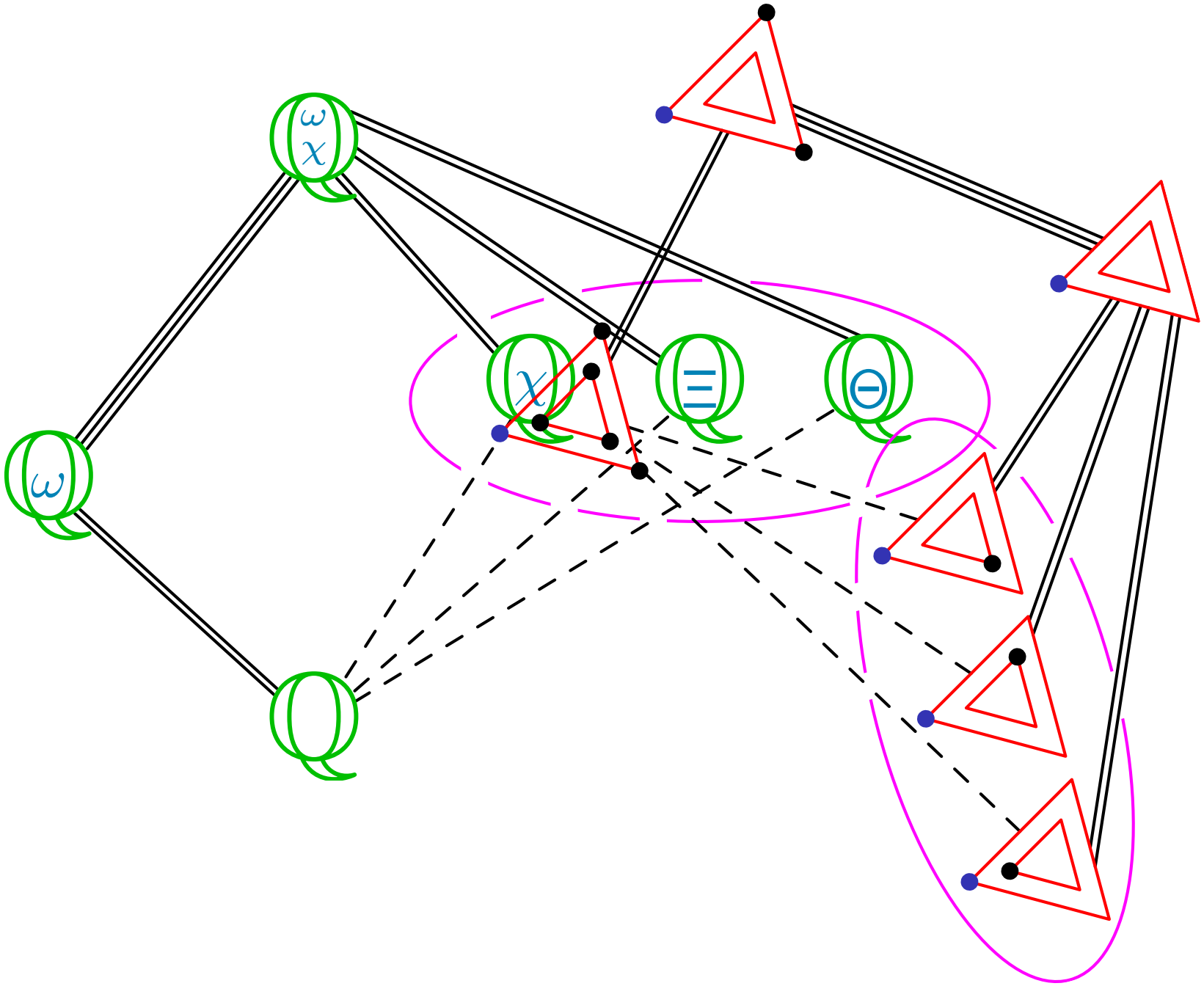

ω
χ
ω
χ
Ξ
Θ

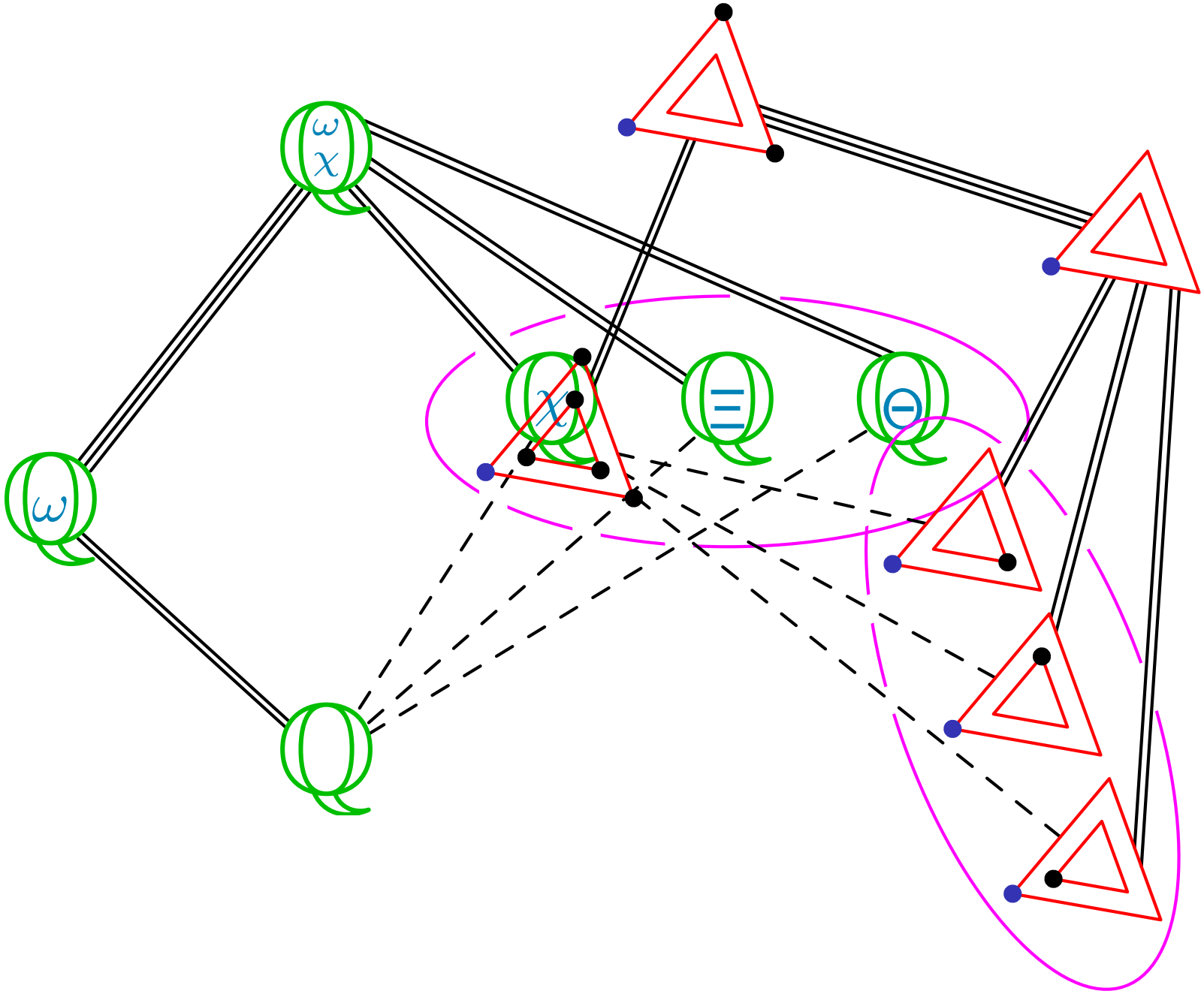

ω
χ
χ
Ξ
Θ
ω

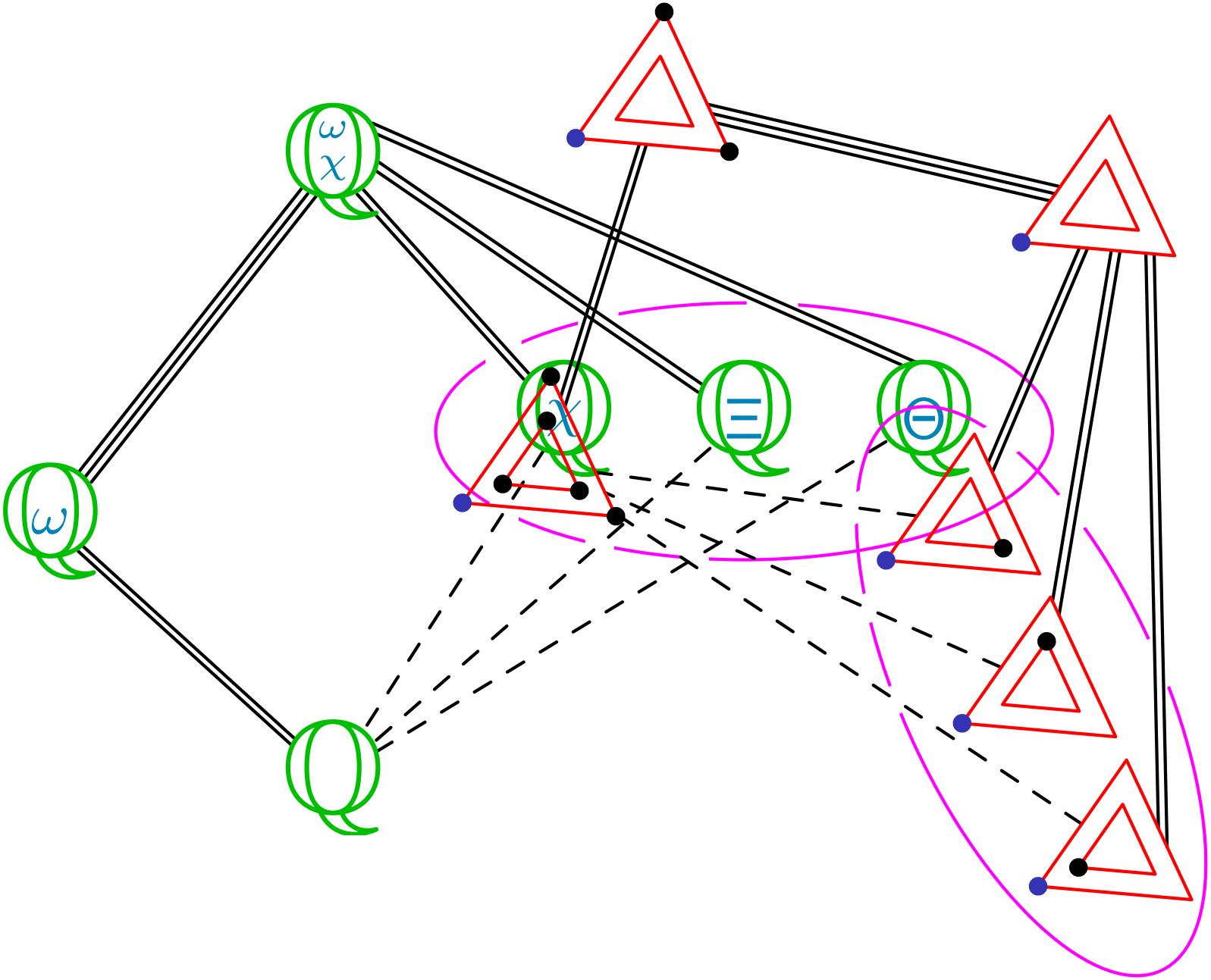

ω
χ
χ
ω
Ξ
Θ

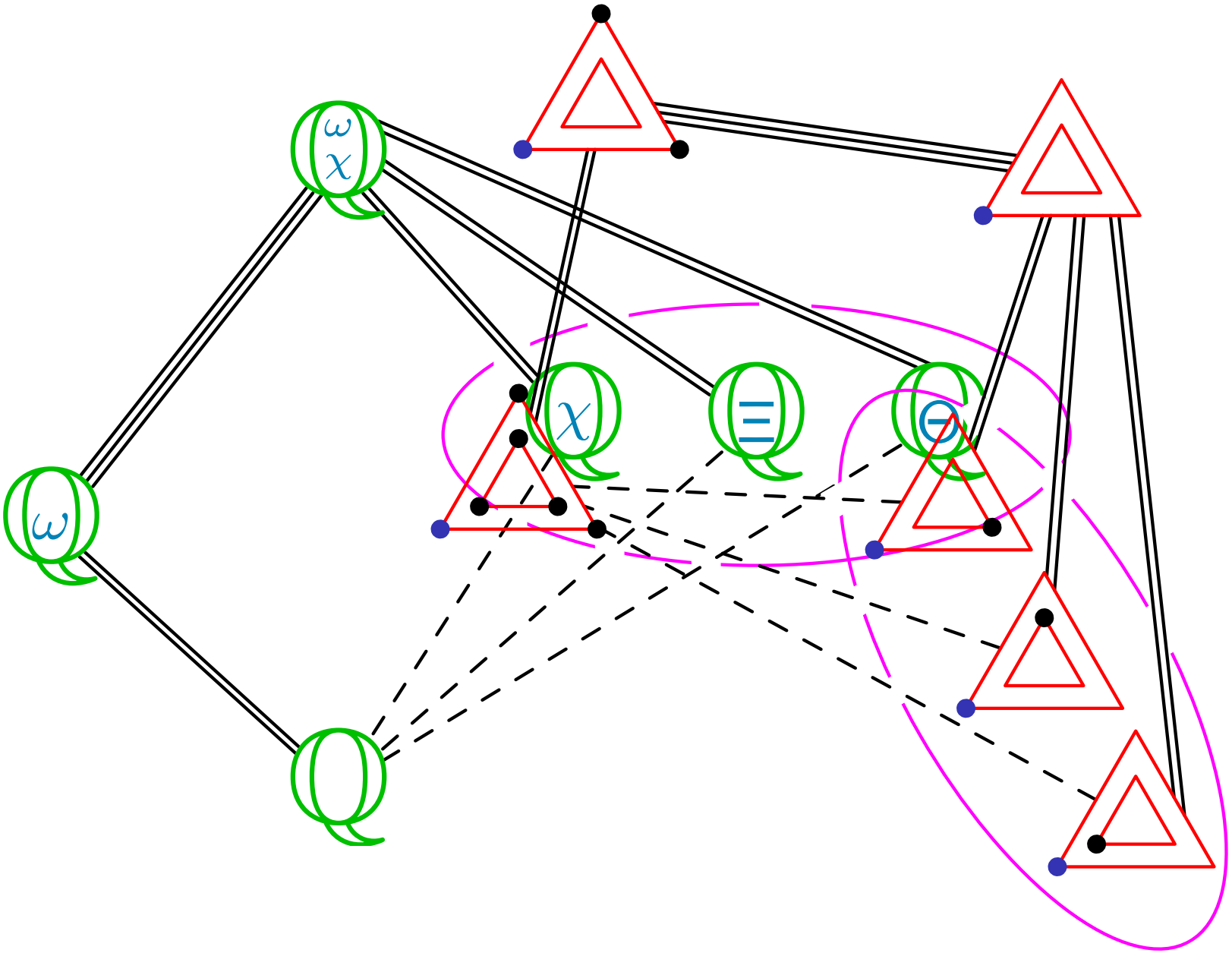

ω
χ
χ
Ξ
Θ
ω

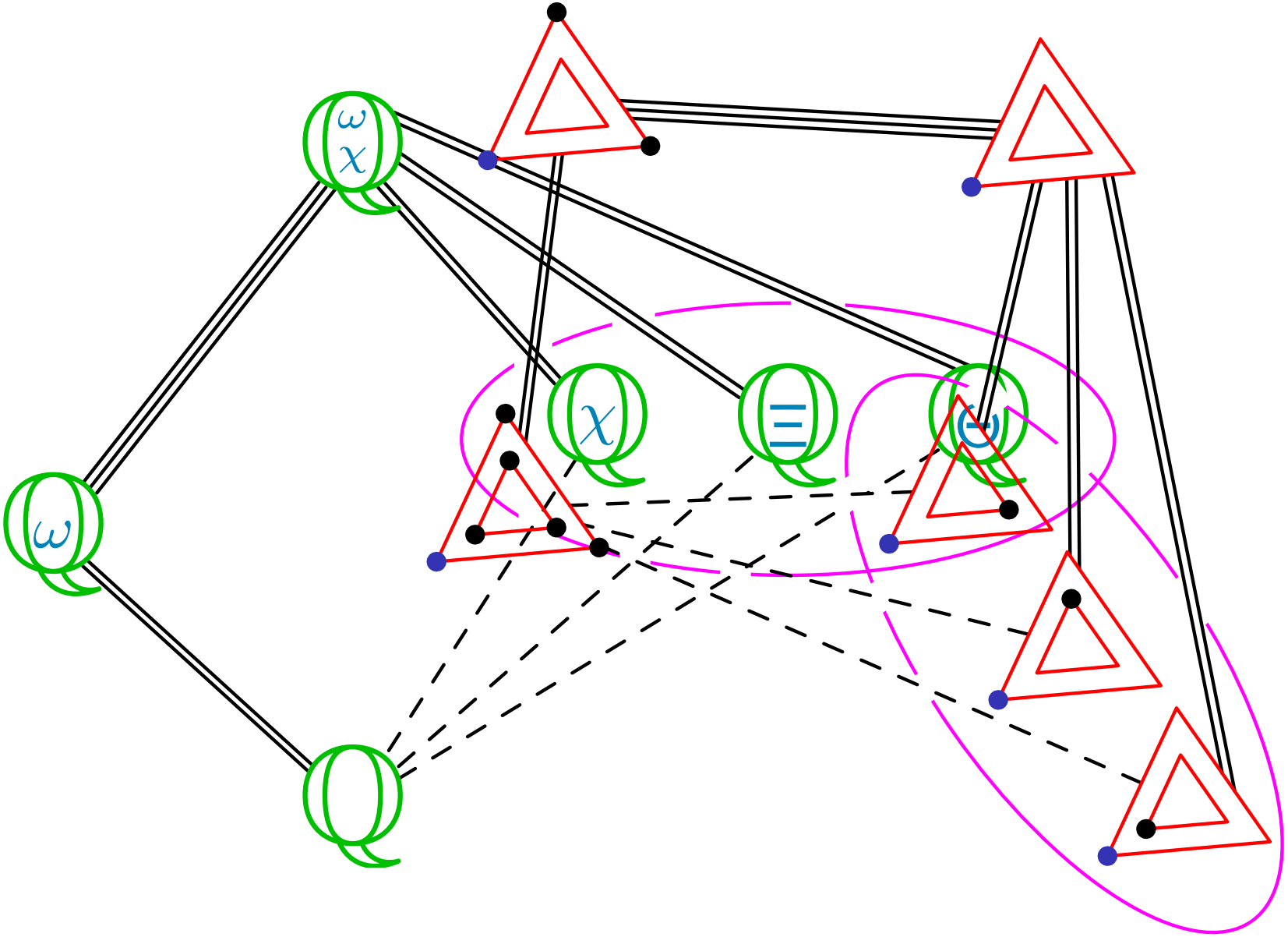

ω
χ
χ
≡
⊖
ω

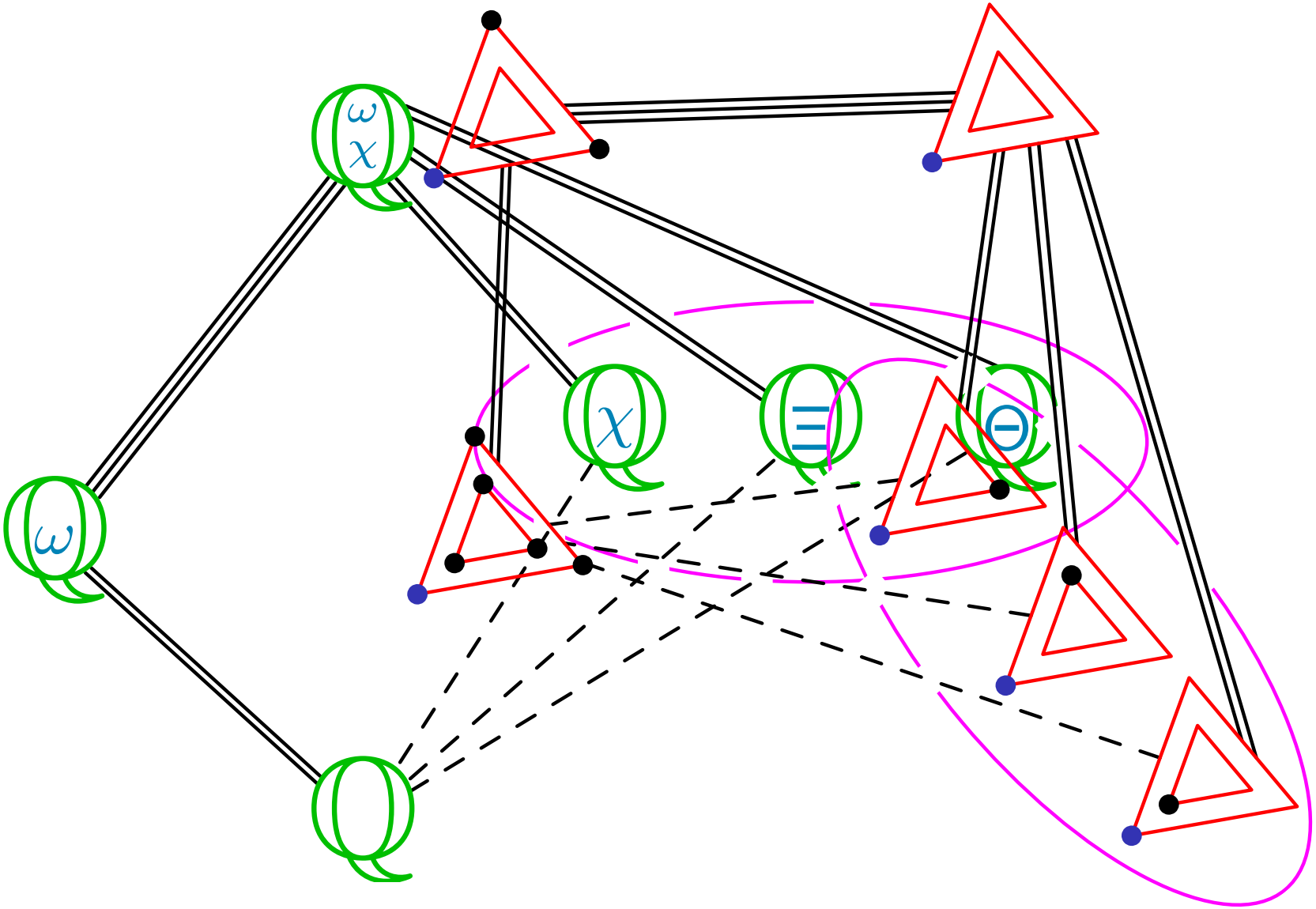

ω
χ
ω
χ
=
⊖

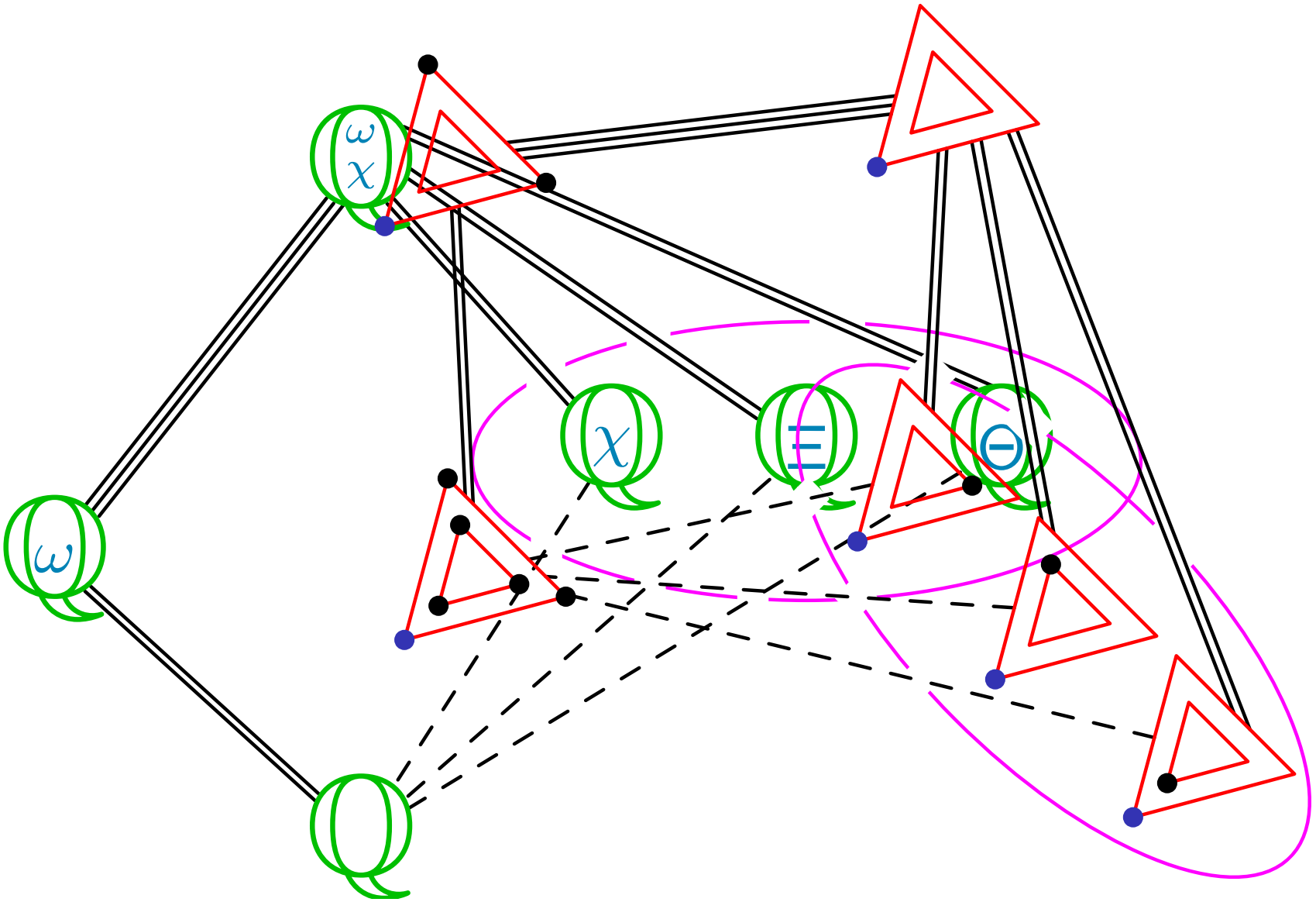

ω
χ
χ
ω
≡
⊖

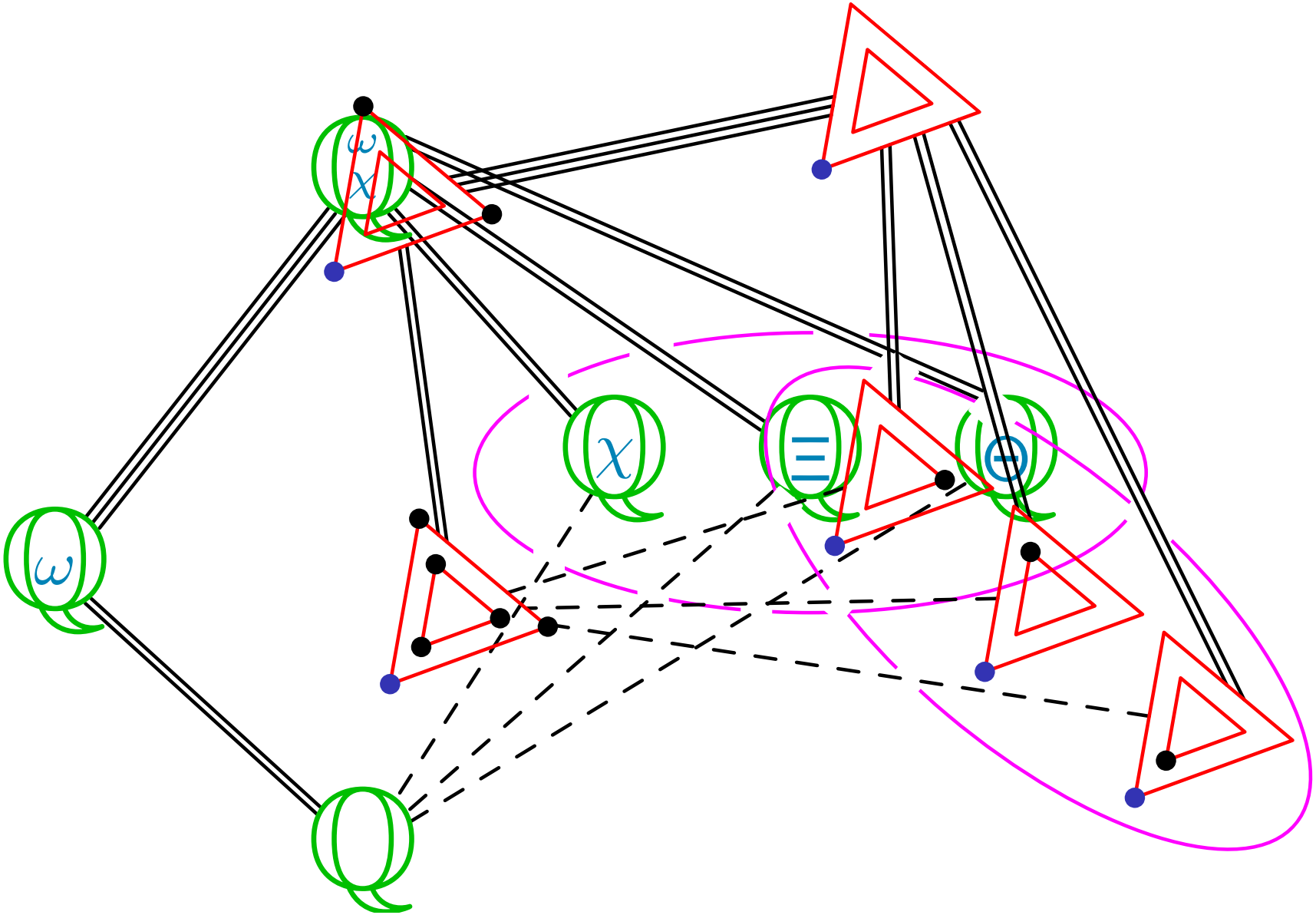

ω
χ
ω
χ
≡
⊖

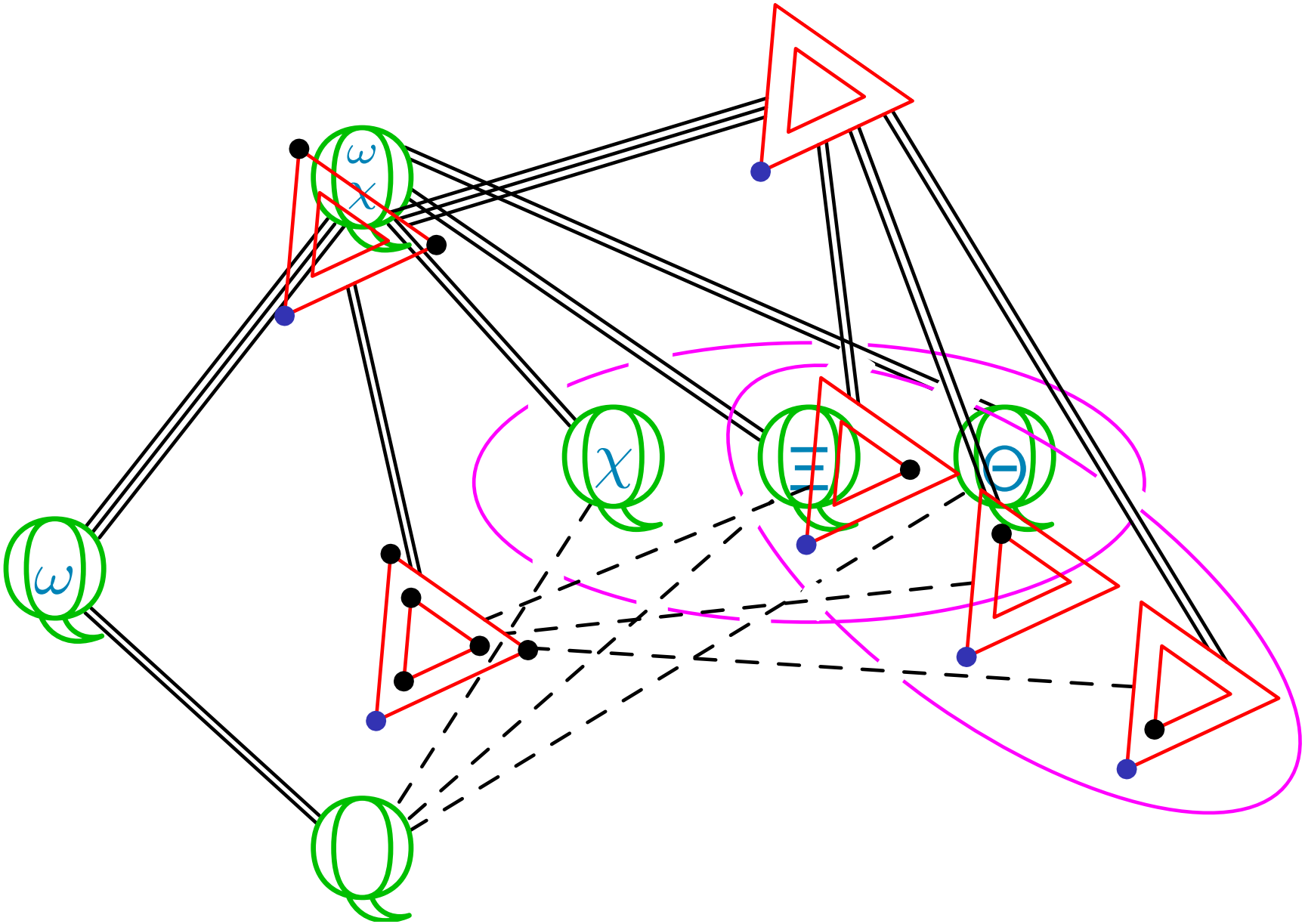

ω
χ
χ
ω

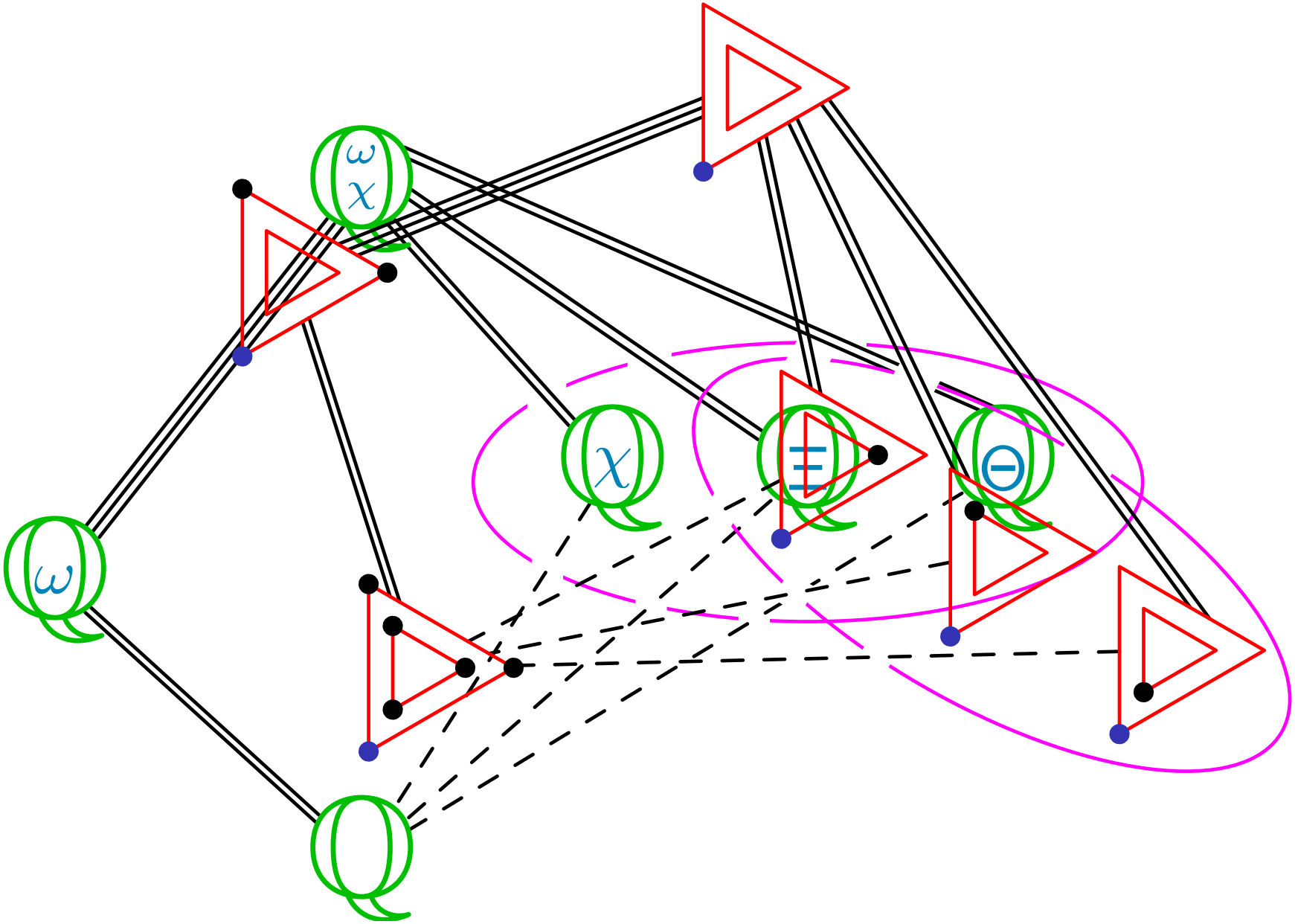

ω
χ
χ
≡
ω

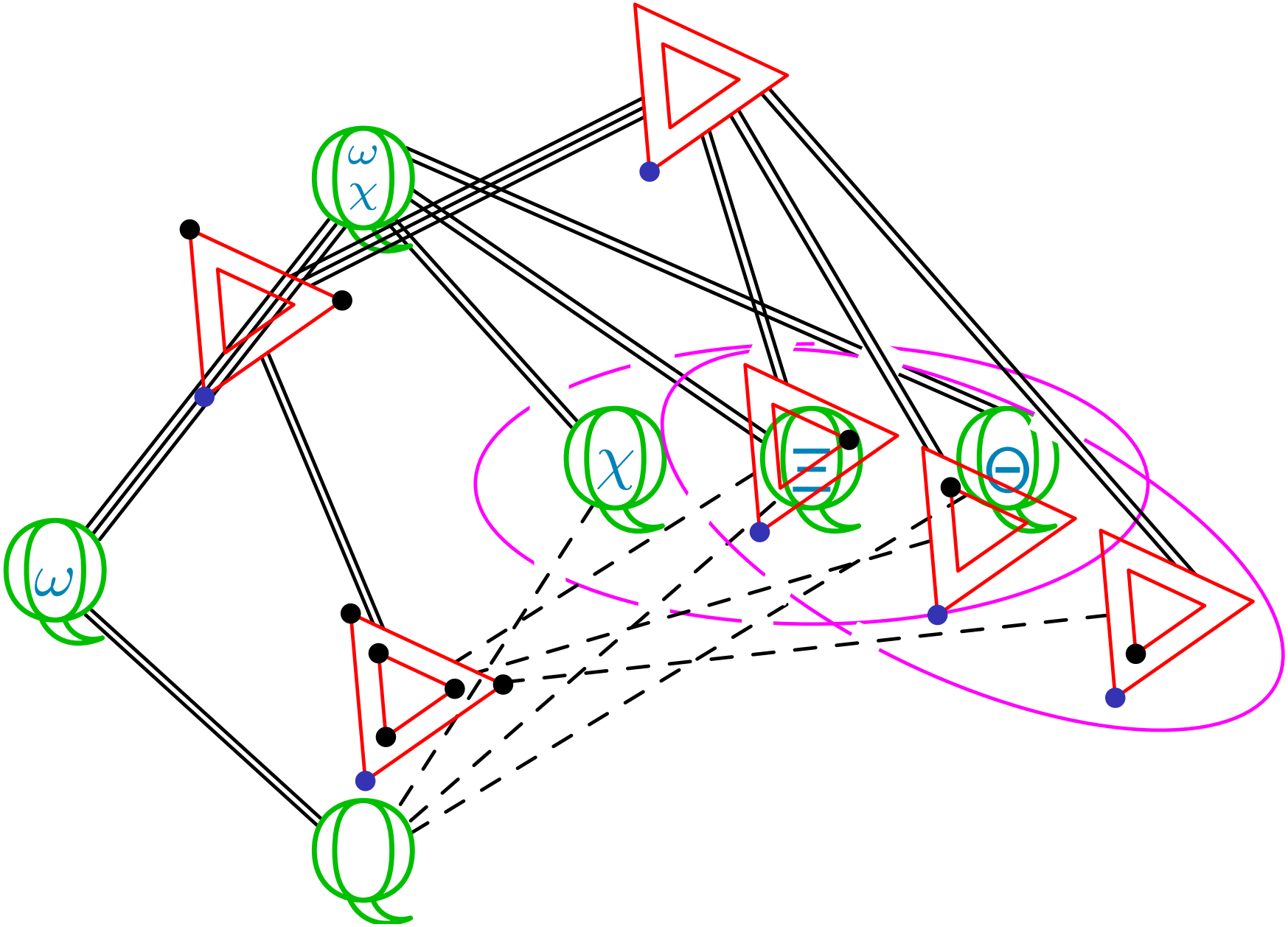

ω
χ
χ
≡
⊖
ω

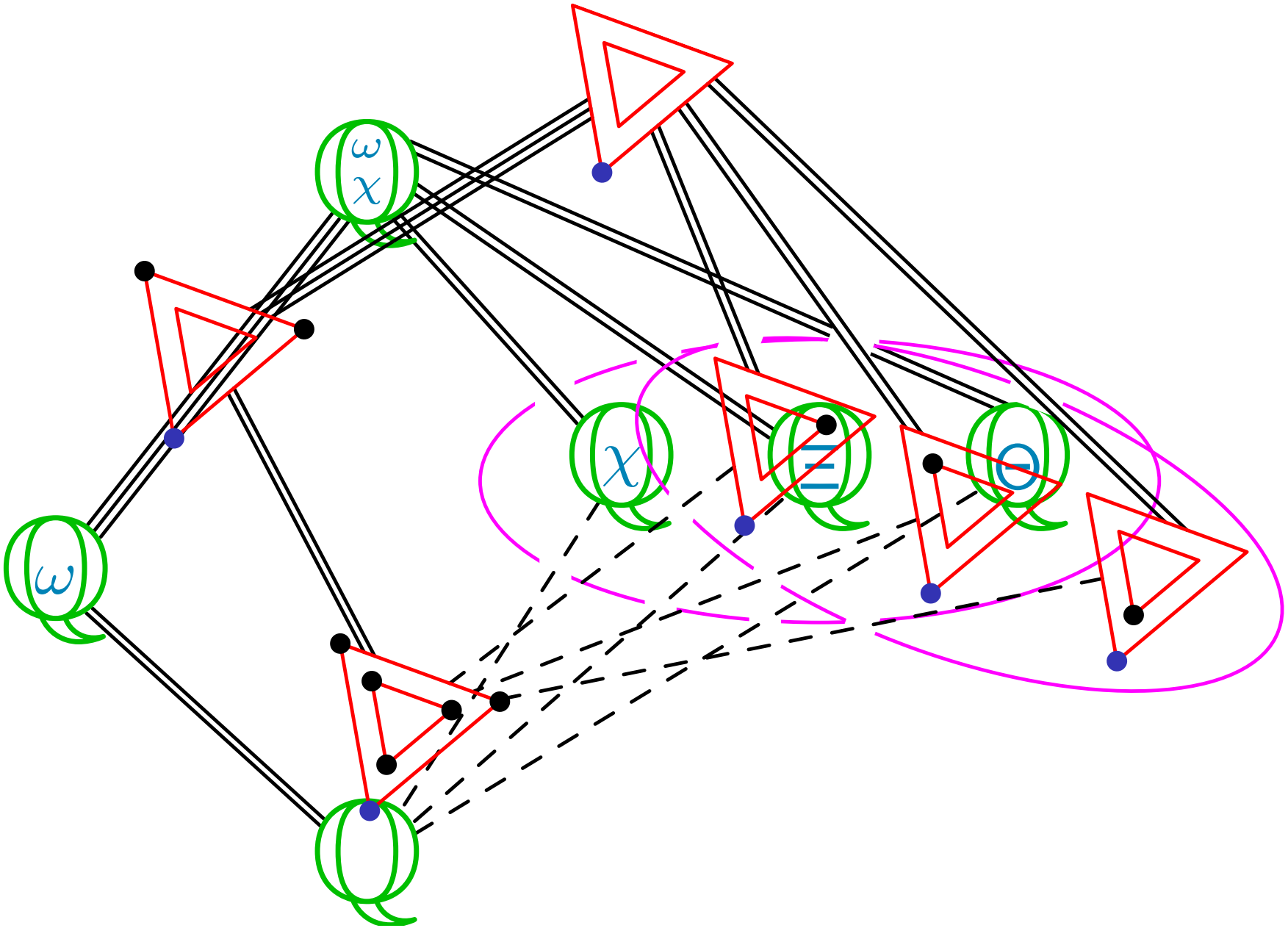

ω
χ
χ
Ξ
Θ
ω

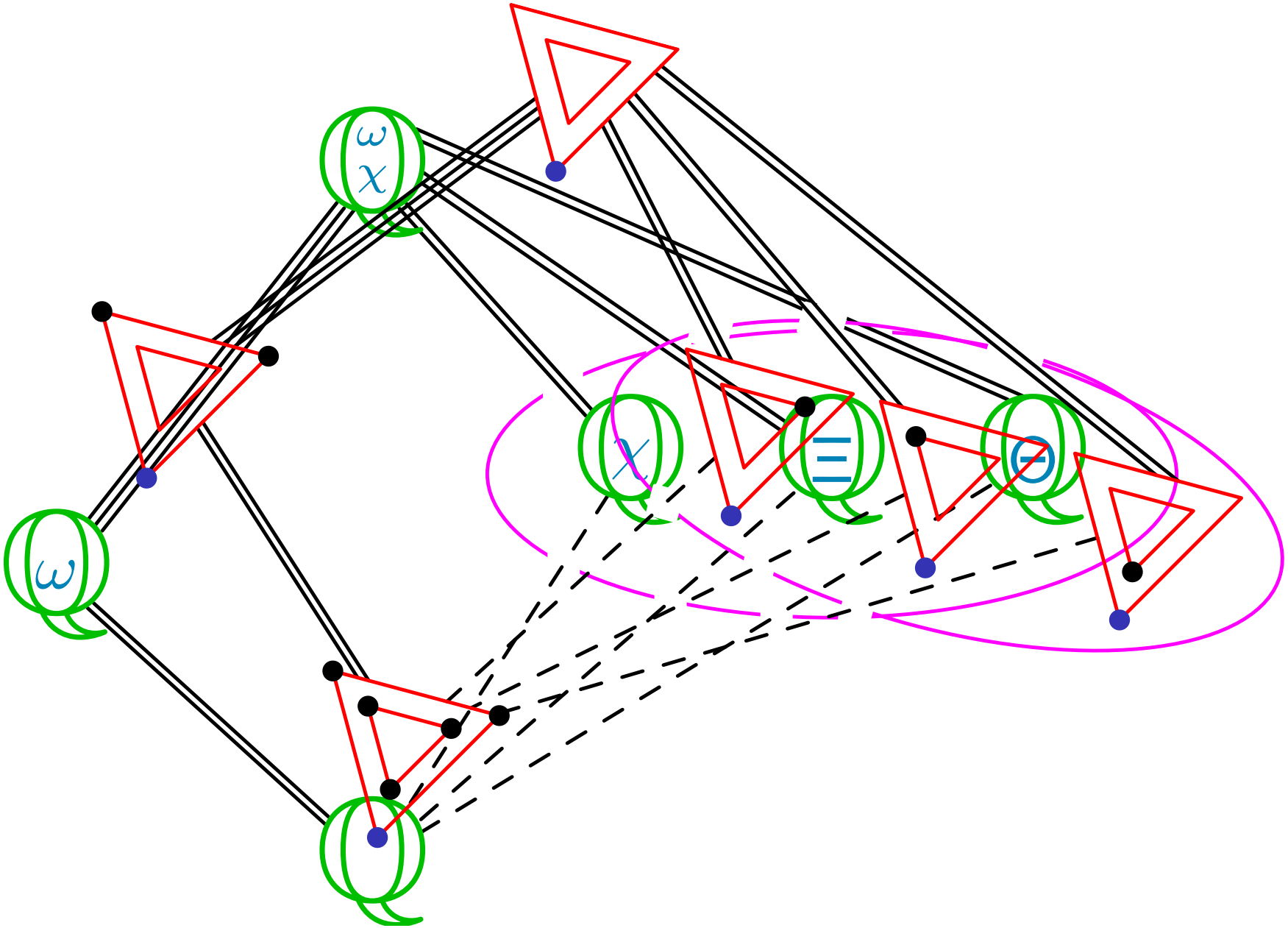

ω
χ
χ
≡
⊖
ω

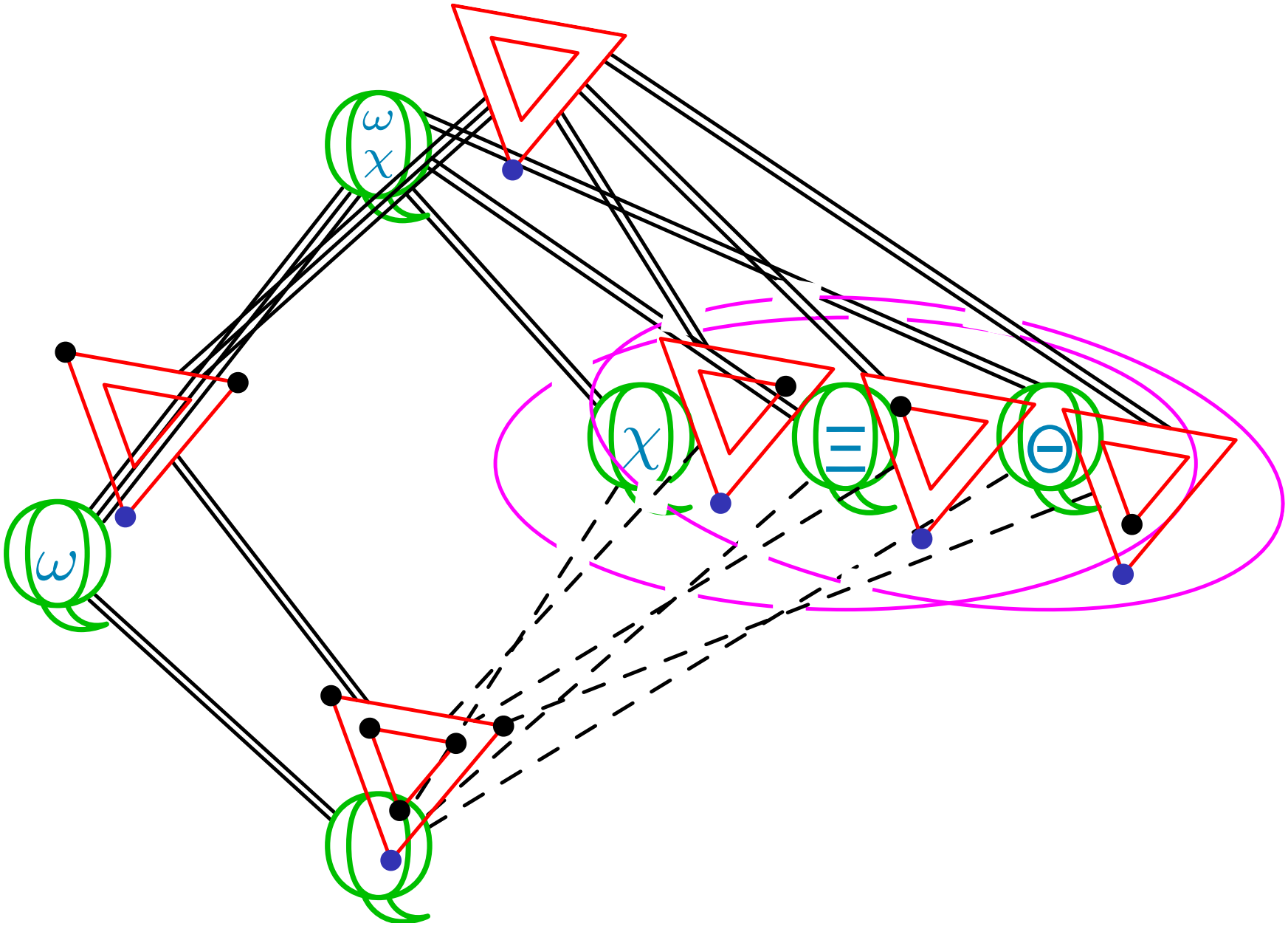

ω
χ
χ
ω

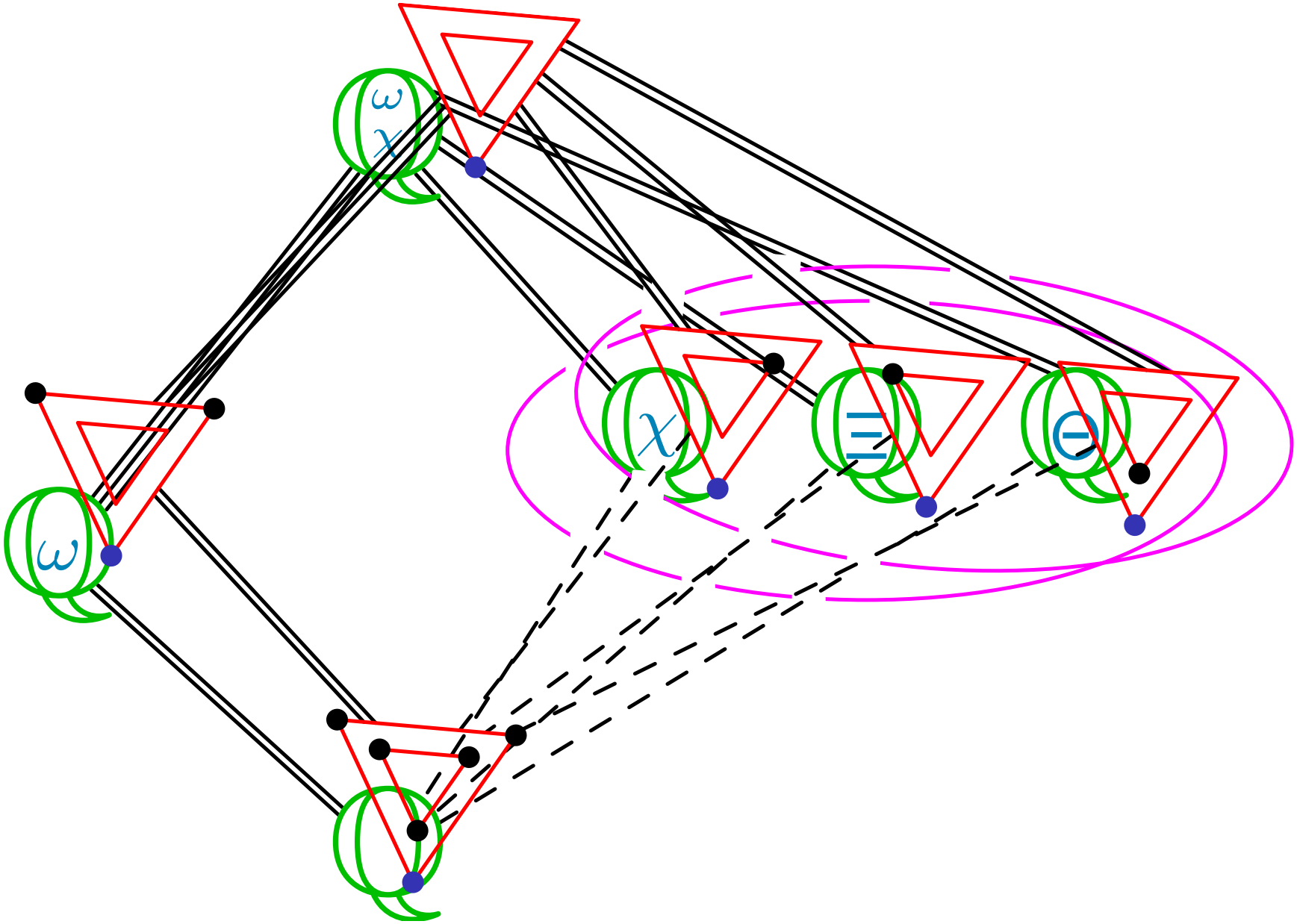

ω
χ
χ
Ξ
Θ
ω

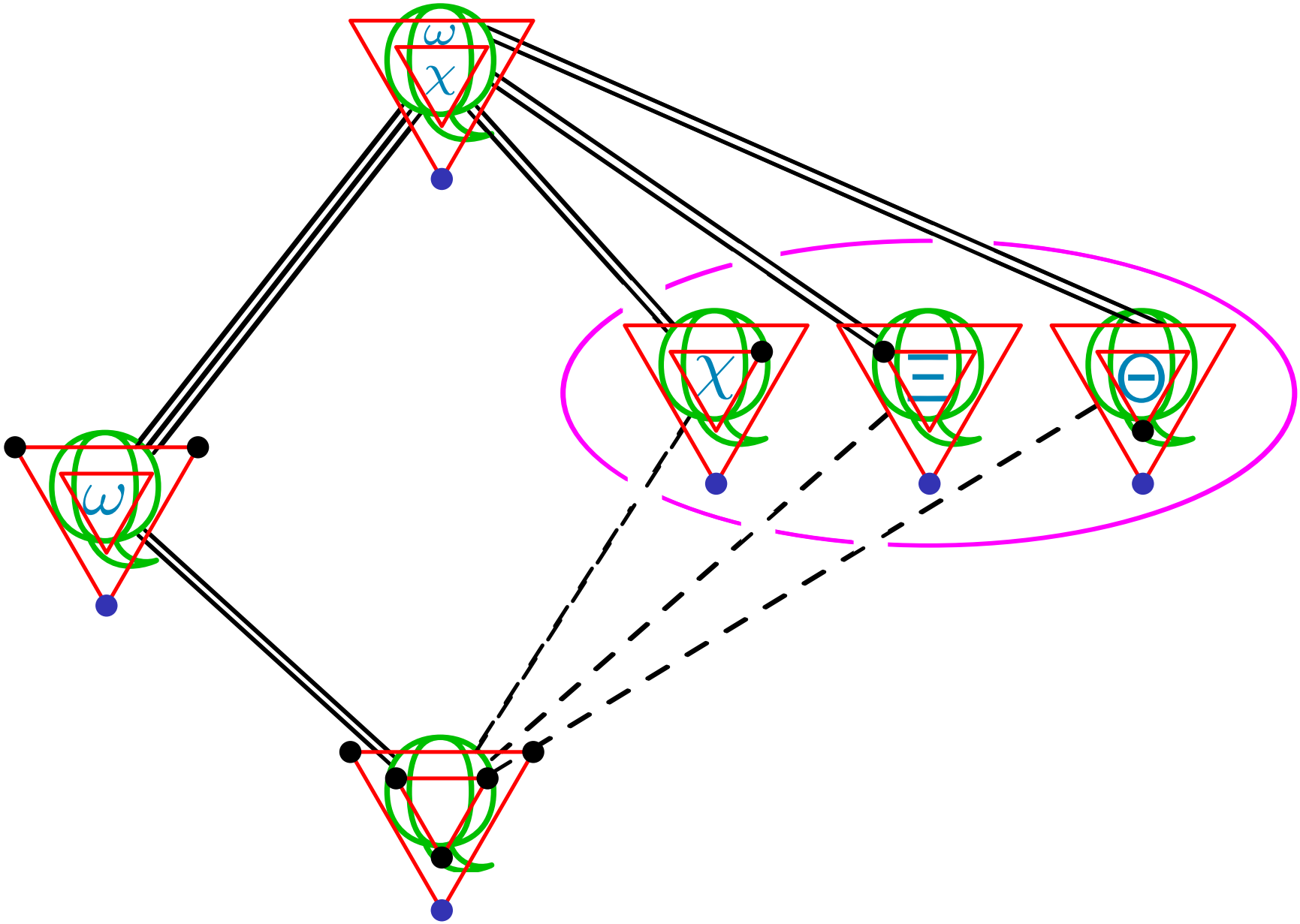

ω
χ
χ
ω

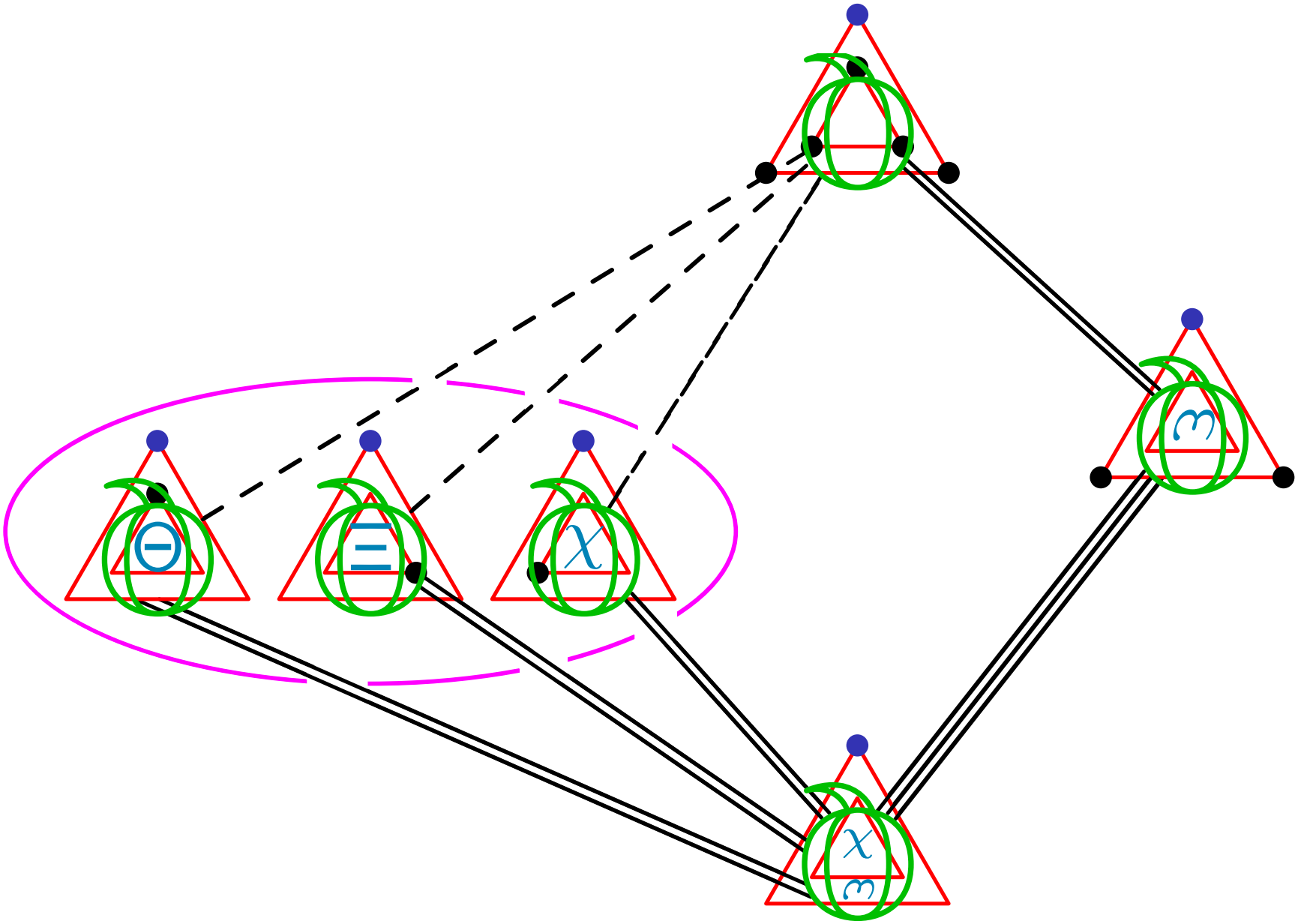

ω
χ
χ
Ξ
Θ
ω


ω
χ
ω
χ
≡
⊖


ω
χ
ω
χ
≡
⊖


ω
χ
ω
χ
≡
⊖

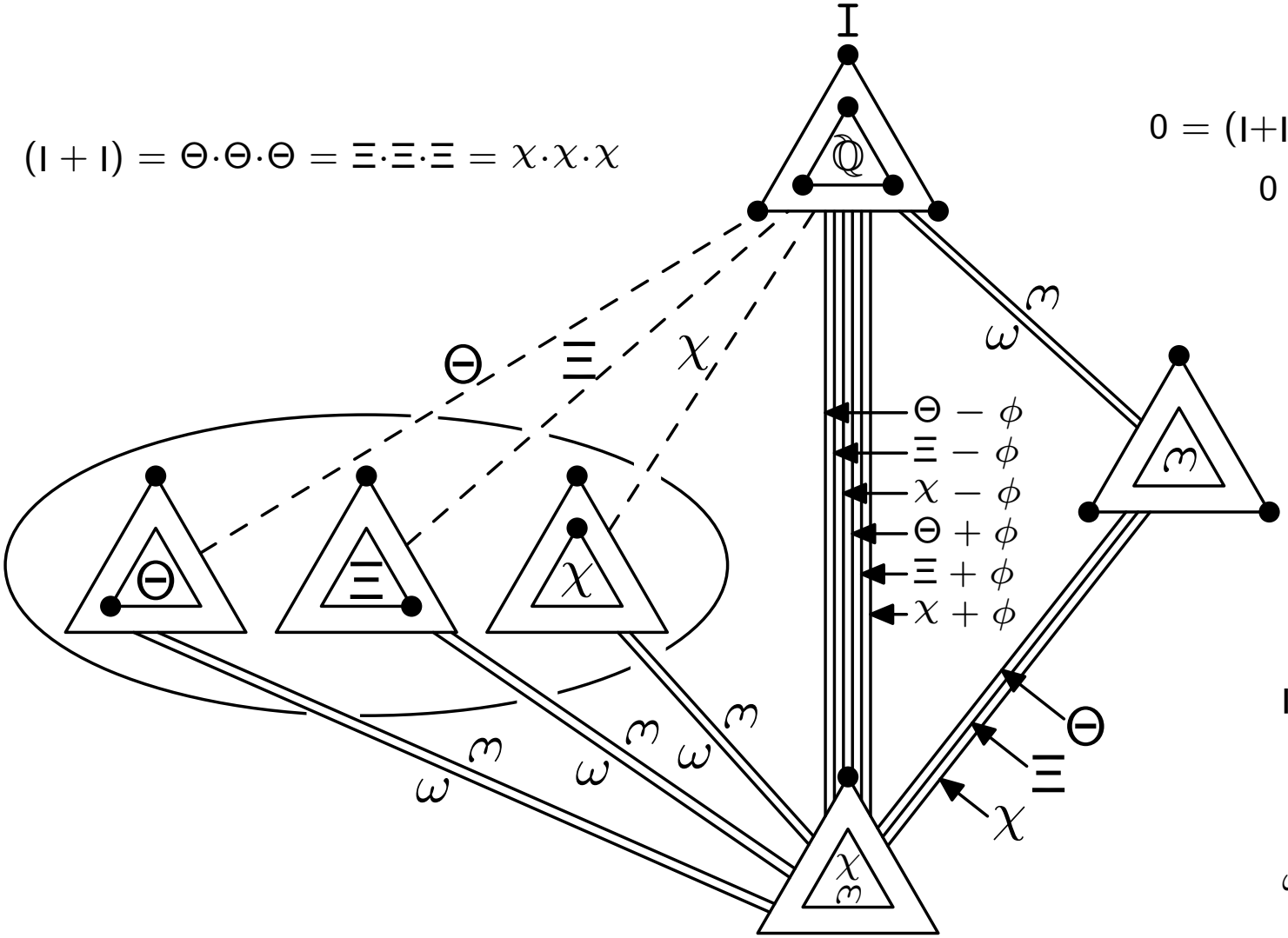

ω
χ
χ
ω


Θ
Ξ
χ
m
χ
m

$(\mathsf{I}+\mathsf{I}) = \Theta\cdot\Theta\cdot\Theta = \Xi\cdot\Xi\cdot\Xi = \chi\cdot\chi\cdot\chi$

$0 = (\mathsf{I}+\mathsf{I}+\mathsf{I}) + \phi\cdot\phi$

$0 = \omega+\mathsf{I}+\mathfrak{m}$



$\mathsf{I} = \mathfrak{m}\cdot\mathfrak{m}\cdot\mathfrak{m}$

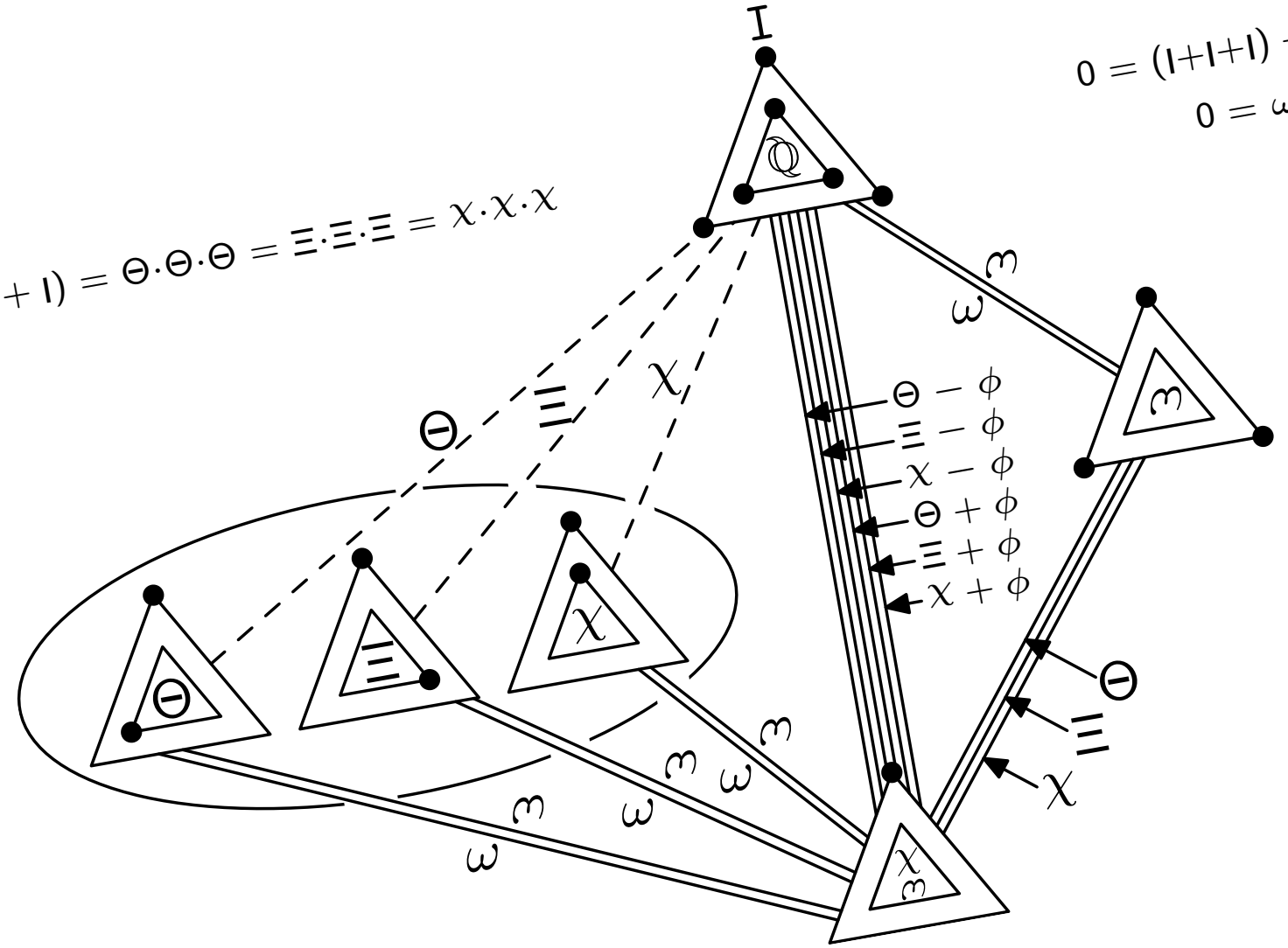
$\omega\cdot\omega = \mathfrak{m}$

$\omega = \mathfrak{m}\cdot\mathfrak{m}$

$\omega\cdot\omega\cdot\omega = \mathsf{I}$

$$0 = (1+1+1) + \phi\cdot\phi$$
$$0 = \omega+1+m$$

$$(1+1) = \Theta\cdot\Theta\cdot\Theta = \Xi\cdot\Xi\cdot\Xi = \chi\cdot\chi\cdot\chi$$



$$1 = m\cdot m\cdot m$$
$$\omega\cdot\omega = m$$
$$\omega = m\cdot m$$
$$\omega\cdot\omega\cdot\omega = 1$$

$0 = (1+1+1) + \phi\cdot\phi$

$0 = \omega+1+\mathfrak{m}$

$(1+1) = \Theta\cdot\Theta\cdot\Theta = \Xi\cdot\Xi\cdot\Xi = \chi\cdot\chi\cdot\chi$

$1 = \mathfrak{m}\cdot\mathfrak{m}\cdot\mathfrak{m}$

$\omega\cdot\omega = \mathfrak{m}$

$\omega = \mathfrak{m}\cdot\mathfrak{m}$

$\omega\cdot\omega\cdot\omega = 1$

$\longleftarrow$

$0 = (1+1)$

$0 = \omega$

$(1+1) = \ominus.\ominus.\ominus = \equiv.\equiv.\equiv = \chi.\chi.\chi$

$1 = \omega.\omega.\omega$

$\omega.\omega = \omega$

$\omega = \omega.\omega$

$\omega.\omega.\omega = 1$

$$(1+1) = \ominus\cdot\ominus\cdot\ominus = \equiv\cdot\equiv\cdot\equiv = \chi\cdot\chi\cdot\chi$$

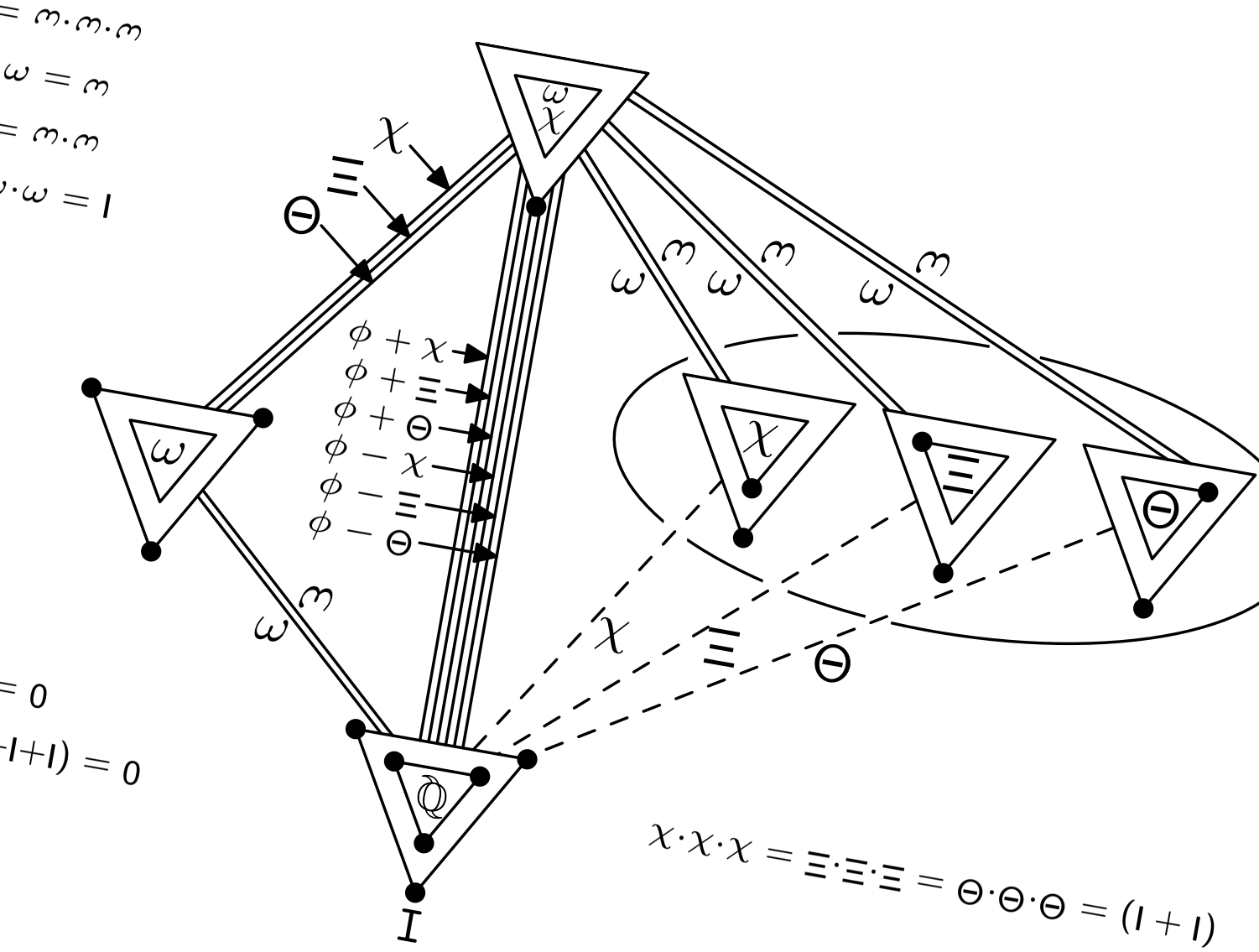
I
ω
ω
ω
ω
ω
ω
ω
ω
χ
χ
χ

$$(1+1) = \ominus\cdot\ominus\cdot\ominus = \equiv\equiv\equiv = \chi\cdot\chi\cdot\chi$$

I
ω
ω
ω
ω
ω
ω
ω
ω
χ
χ
χ

$$(1+1) = \Theta\cdot\Theta\cdot\Theta = \equiv\cdot\equiv\cdot\equiv = \chi\cdot\chi\cdot\chi$$

I
Θ
χ
ω
ω
ω

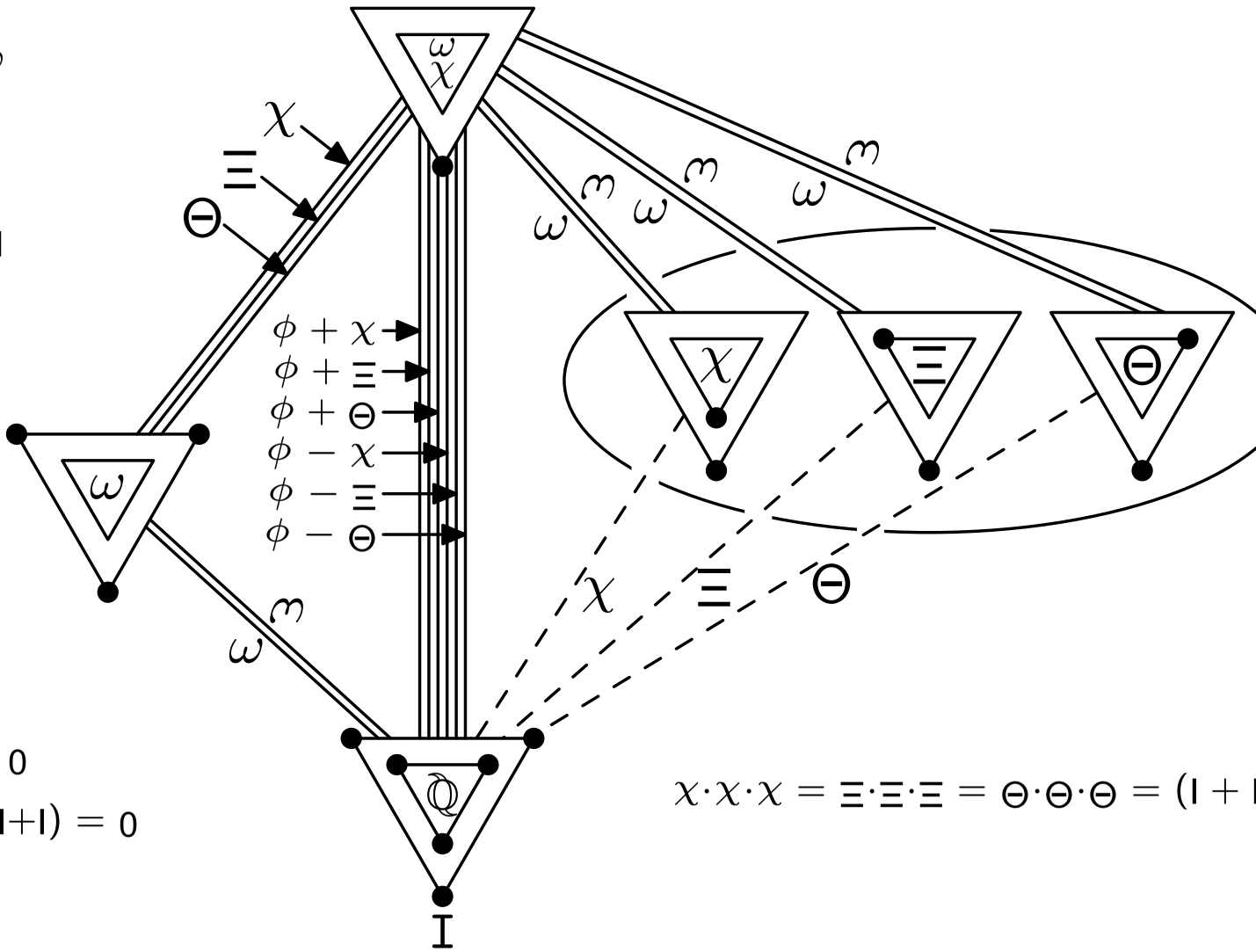

$= \mathfrak{m}\cdot\mathfrak{m}\cdot\mathfrak{m}$
$\omega = \mathfrak{m}$
$= \mathfrak{m}\cdot\mathfrak{m}$
$\cdot\omega = 1$
χ
Ξ
Θ
ω
$\mathfrak{m}$
$\phi + \chi$
$\phi + \Xi$
$\phi + \Theta$
$\phi - \chi$
$\phi - \Xi$
$\phi - \Theta$
$= 0$
$-1+1) = 0$
$\mathbb{Q}$
I
$\chi\cdot\chi\cdot\chi = \Xi\cdot\Xi\cdot\Xi = \Theta\cdot\Theta\cdot\Theta = (1+1)$

$\omega\cdot\omega$

$= \omega$

$\cdot\omega$

$= \mathsf{I}$



$\omega = 0$

$(\mathsf{I}+\mathsf{I}+\mathsf{I}) = 0$

$\chi\cdot\chi\cdot\chi = \Xi\cdot\Xi\cdot\Xi = \Theta\cdot\Theta\cdot\Theta = (\mathsf{I} + \mathsf{I}$

$\downarrow$

$\chi\cdot\chi\cdot\chi\cdot\chi = \text{III}\cdot\text{III}\cdot\text{III}\cdot\text{III} = \text{I}\cdot\text{I}\cdot\text{I}\cdot\text{I} = 1$
$0 = (1+1+1) + 0 + 0 + 0$
$0 = 3 + 1 + 1 + 1$
$1 = 1 + 1 + 1 +

$$\phi \cdot \phi + (1+1+1) = 0$$

$$1+1+3 = 0$$

1
2
3
3
3

$\phi \cdot \phi + (1+1+1) = 0$

$\omega + 1 + 3 = 0$

3
3
3

$\omega + 1 + 3 = 0$

$\phi \cdot \phi + (1 + 1 + 1) = 0$

$\chi \cdot \chi \cdot \chi = \equiv \equiv \equiv = \odot \cdot \odot \cdot \odot = 1$

$= 1$

$\omega + 1 + m = 0$

$\phi \cdot \phi + (1+1+1) = 0$

$\omega \cdot \omega = 1$

$\chi \cdot \chi \cdot \chi = \equiv \cdot \equiv \cdot \equiv = \Theta \cdot \Theta \cdot \Theta = (1+1)$

$\omega \cdot \omega \cdot \omega = 1$

$\omega \cdot \mathfrak{m} = \mathfrak{m} \cdot \mathfrak{m}$

$\omega + 1 + \mathfrak{m} = 0$

$\phi \cdot \phi + (1+1+1) = 0$

$\chi \cdot \chi \cdot \chi = \Xi \cdot \Xi \cdot \Xi = \Theta \cdot \Theta \cdot \Theta = (1+1)$

$\omega\cdot\omega\cdot\omega = 1$

$\omega = \mathfrak{m}\cdot\mathfrak{m}$

$\omega\cdot\omega = \mathfrak{m}$

$\mathfrak{m}\cdot\mathfrak{m}\cdot\mathfrak{m}$

$\omega + 1 + \mathfrak{m} = 0$

$\phi\cdot\phi + (1+1+1) = 0$

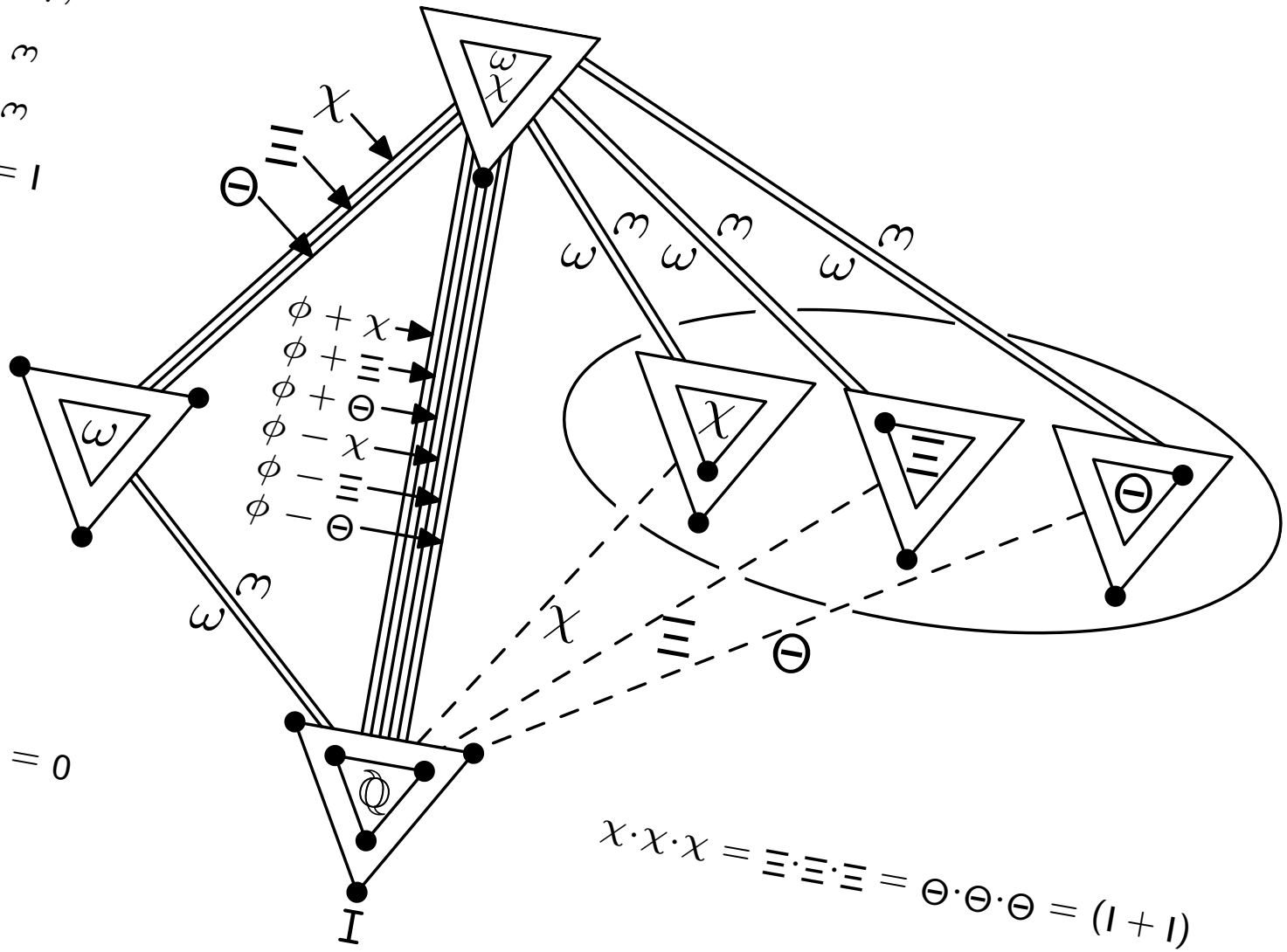
$\chi\cdot\chi\cdot\chi = \equiv\cdot\equiv\cdot\equiv = \Theta\cdot\Theta\cdot\Theta = (1+1)$

$$\mathcal{I} = \mathfrak{m}\cdot\mathfrak{m}\cdot\mathfrak{m}$$

$$\omega\cdot\omega = \mathfrak{m}$$

$$\omega = \mathfrak{m}\cdot\mathfrak{m}$$

$$\omega\cdot\omega\cdot\omega = \mathcal{I}$$



$$\omega + \mathcal{I} + \mathfrak{m} = 0$$

$$\phi\cdot\phi + (\mathcal{I}+\mathcal{I}+\mathcal{I}) = 0$$

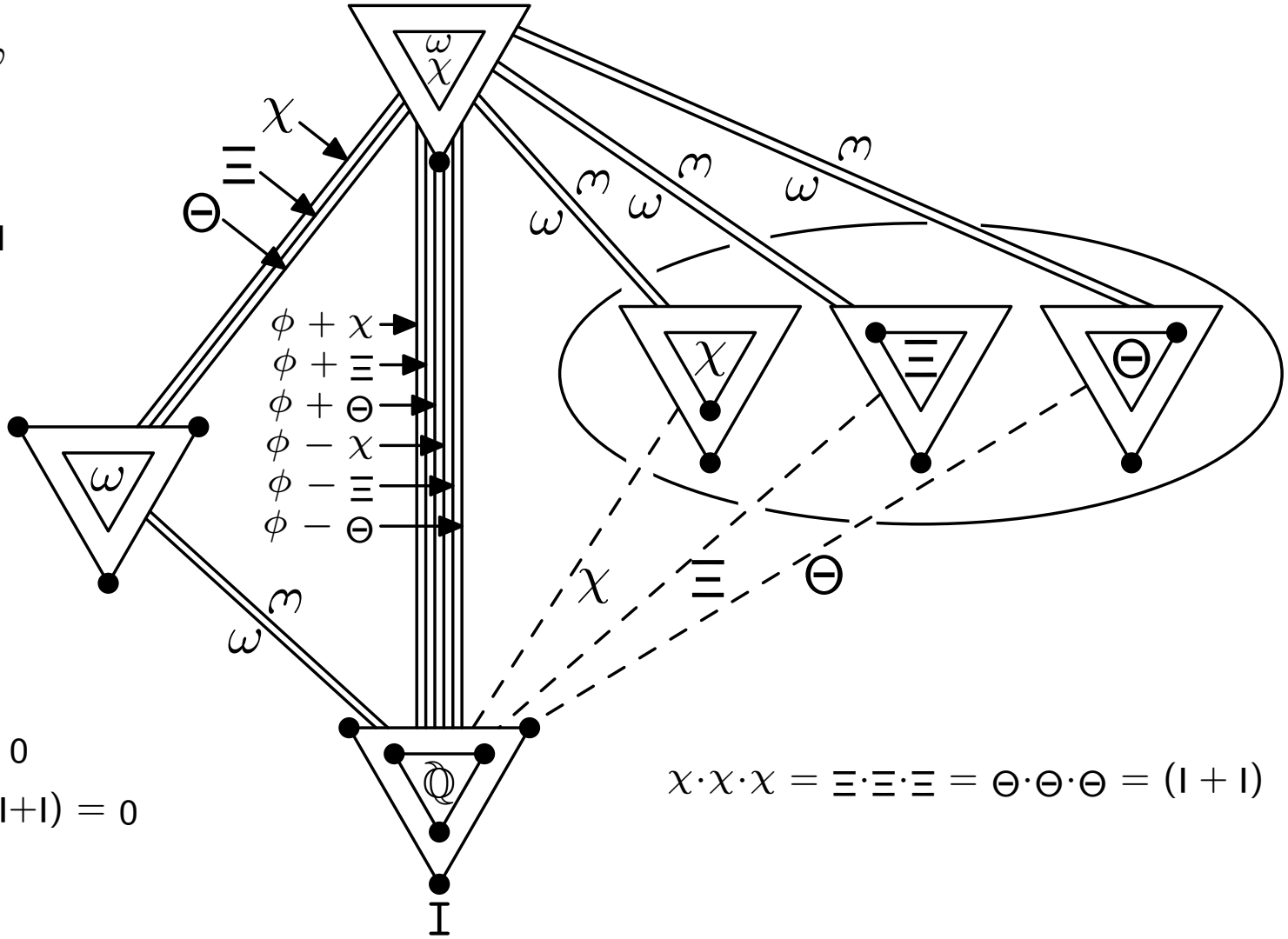
$$\chi\cdot\chi\cdot\chi = \Xi\cdot\Xi\cdot\Xi = \Theta\cdot\Theta\cdot\Theta = (\mathcal{I}+\mathcal{I})$$

$\mathsf{I} = \mathfrak{m}\cdot\mathfrak{m}\cdot\mathfrak{m}$

$\omega\cdot\omega = \mathfrak{m}$

$\omega = \mathfrak{m}\cdot\mathfrak{m}$

$\omega\cdot\omega\cdot\omega = \mathsf{I}$



$\omega + \mathsf{I} + \mathfrak{m} = 0$

$\phi\cdot\phi + (\mathsf{I}+\mathsf{I}+\mathsf{I}) = 0$

$\chi\cdot\chi\cdot\chi = \Xi\cdot\Xi\cdot\Xi = \Theta\cdot\Theta\cdot\Theta = (\mathsf{I}+\mathsf{I})$

Le théorème fondamental de (la théorie de) Galois

Le treillis des extensions de corps entre $\mathbb{Q}$ et le corps de décomposition K d'un polynôme donné $f(x)$ *est isomorphe au treillis des sous-groupes* du groupe G de symétries des racines de $f(x)$ — pourvu que l'un des treillis soit retourné par rapport à l'autre.

Si H est un sous-groupe de G qui correspond au corps intermédiaire F, alors chaque élément de H est une symétrie (un automorphisme) de K qui laisse invariant tous les éléments de F.

Chaque *sous-groupe distingué* correspond à une *extension galoisienne.* Et chaque famille de *sous-groupes conjugués* correspond à une famille *d'extensions conjuguées.*

La correspondance de Galois

Le groupe de Galois de $f(x)$

$$\begin{array}{ccc} G & \longleftrightarrow & \mathbb{Q} \\ | & & | \\ \vdots & & \vdots \\ H & \longleftrightarrow & F \\ \vdots & & \vdots \\ | & & | \\ \{I\} & \longleftrightarrow & K \end{array}$$

Le corps de décomposition de $f(x)$

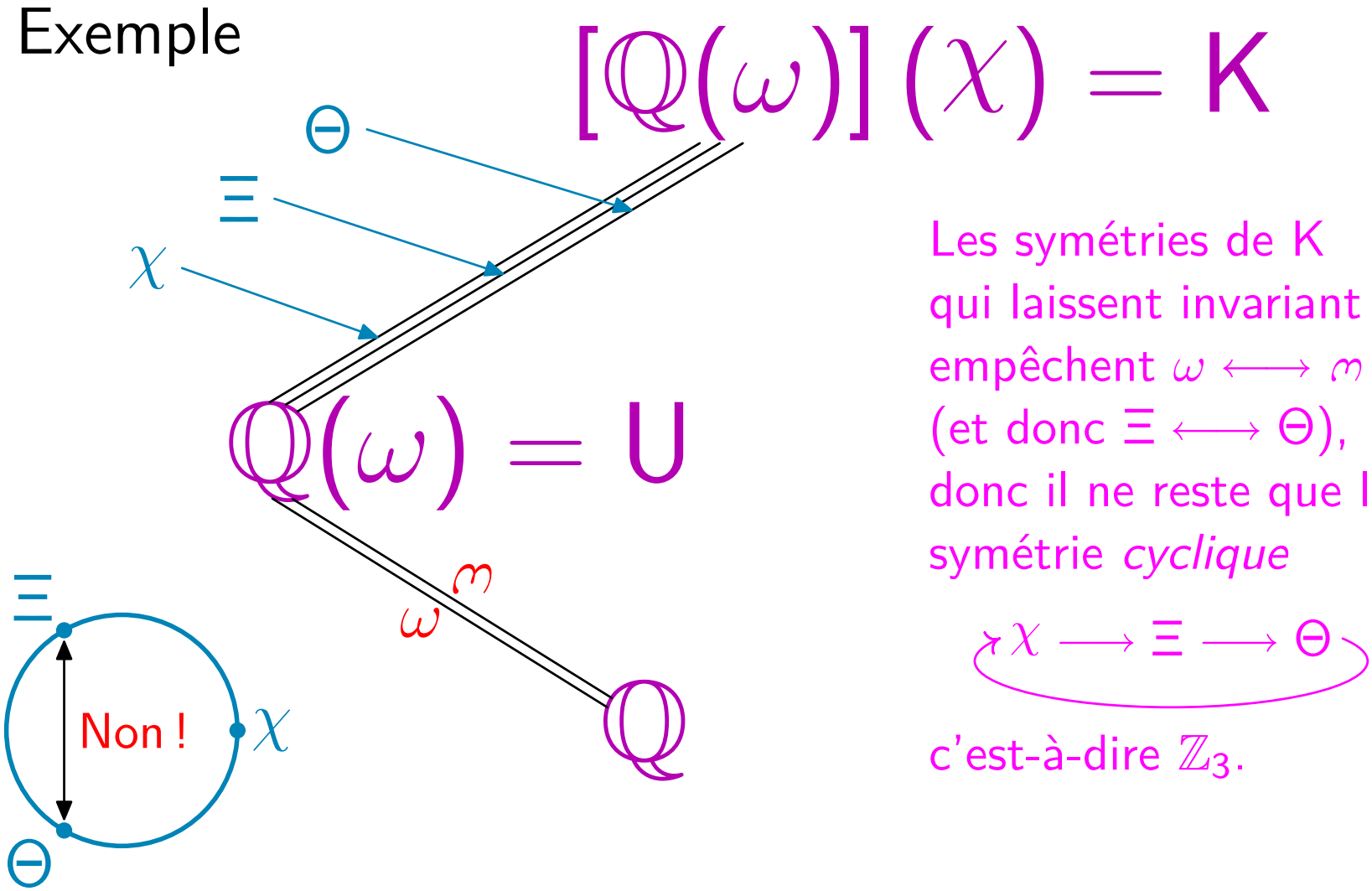
Retour aux équations polynomiales et à la question cruciale de leur résolubilité (ou non !) à l'aide des clés les plus simples (les radicaux : $\sqrt[n]{a}$).

Découverte de Galois :

au radical $\sqrt[p]{a}$ correspond le groupe $\mathbb{Z}_p$

La correspondance des *groupes cycliques* $\mathbb{Z}_p$ aux extensions radicales par $\sqrt[p]{a}$

Exemple



Les symétries de K qui laissent invariant U empêchent $\omega \longleftrightarrow \mathcal{M}$ (et donc $\Xi \longleftrightarrow \Theta$), donc il ne reste que la symétrie *cyclique*

$$\chi \longrightarrow \Xi \longrightarrow \Theta$$

c'est-à-dire $\mathbb{Z}_3$.

Généralisation clé :

Une extension radicale

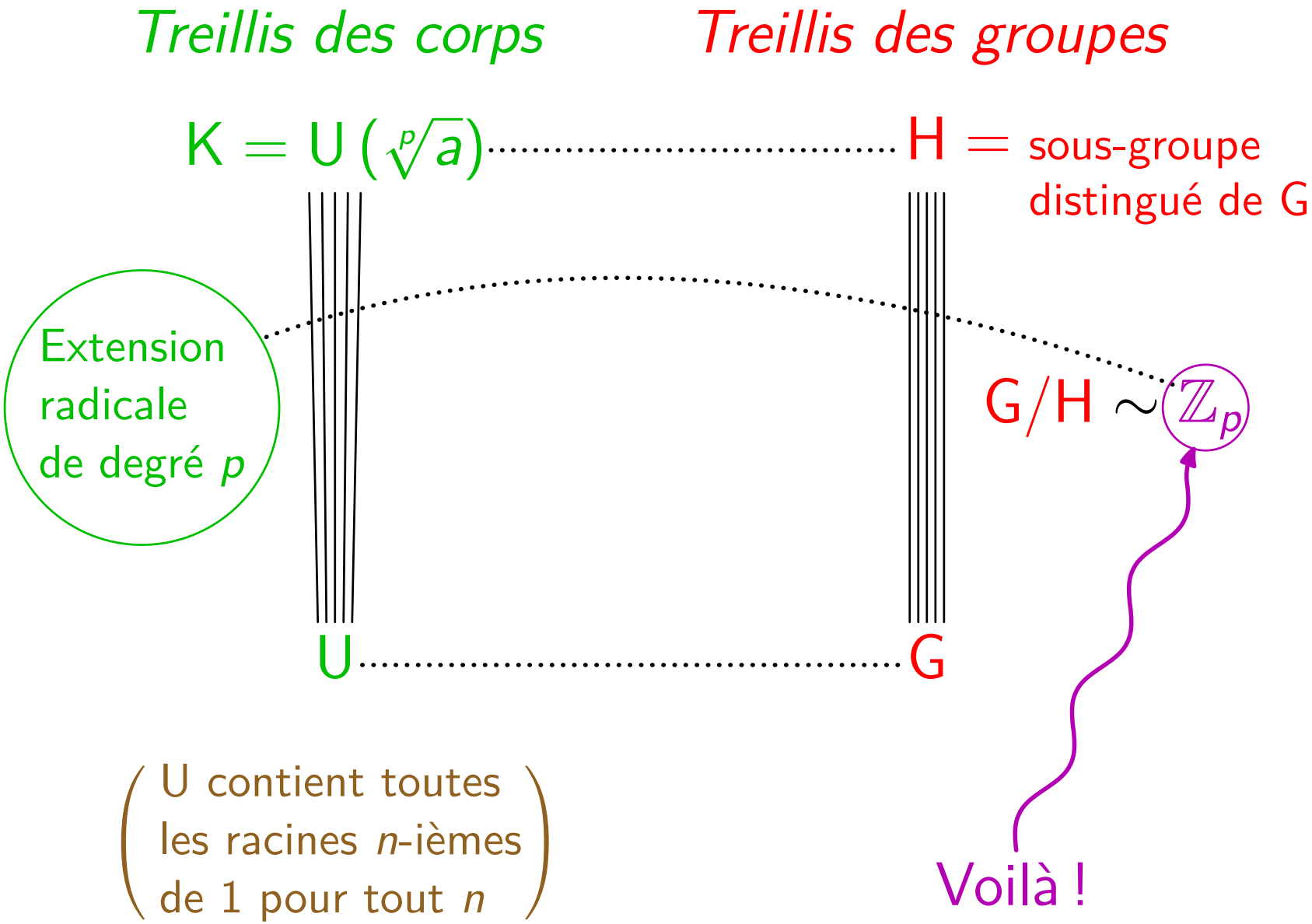
$$\mathrm{U} \longrightarrow \mathrm{K} = \mathrm{U}\left(\sqrt[p]{a}\right) \quad (a \in \mathrm{U})$$

correspond au groupe de symétries $\mathbb{Z}_p$.

Traduction clé au treillis isomorphe :

Dans le treillis des sous-groupes, c'est le *groupe quotient* des deux sous-groupes qui correspondent à U et à K.

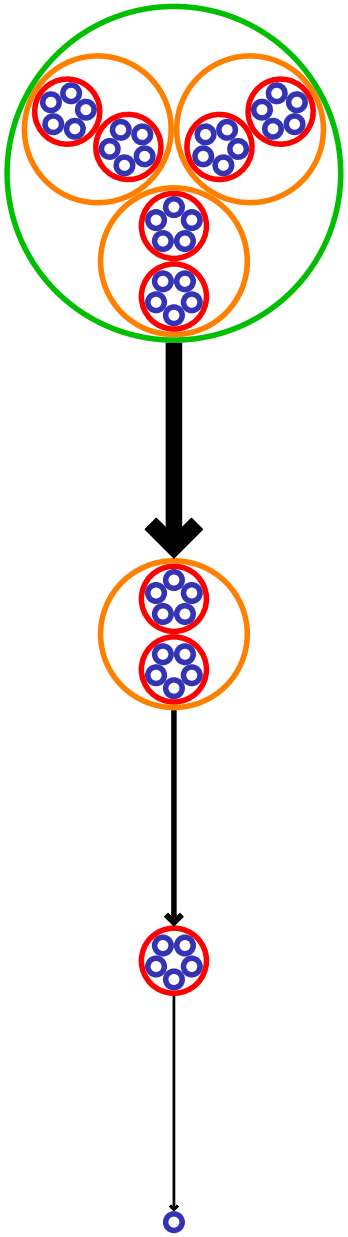
Le signe révélateur d'une extension radicale



Le secret galoisien de la résolubilité d'une équation

Une équation polynomiale résoluble à l'aide de racines de divers degrés correspond à un groupe G de symétries qui possède *une chaîne descendante*, depuis G jusqu'à $\{I\}$, *de sous-groupes distingués* l'un dans l'autre, et *dont les groupes quotient ont tous la forme* $\mathbb{Z}_p$.

Le diagramme de Cayley de G a une structure récursive qui est facilement reconnaissable (des cycles dans des cycles dans des cycles...)



G (30 éléments)

$[G/G' \sim \mathbb{Z}_3]$

G′ (10 éléments)

$[G'/G'' \sim \mathbb{Z}_2]$

G″ (5 éléments)

$[G''/G''' \sim \mathbb{Z}_5]$

G‴ (1 élément)

Pour l'équation *quartique* la plus générale, il y a symétrie totale des 4 racines. Il s'agit donc du groupe S_4 à 24 éléments — le groupe des symétries d'un *cube* (les 4 diagonales sont permutées de toutes les façons possibles) :

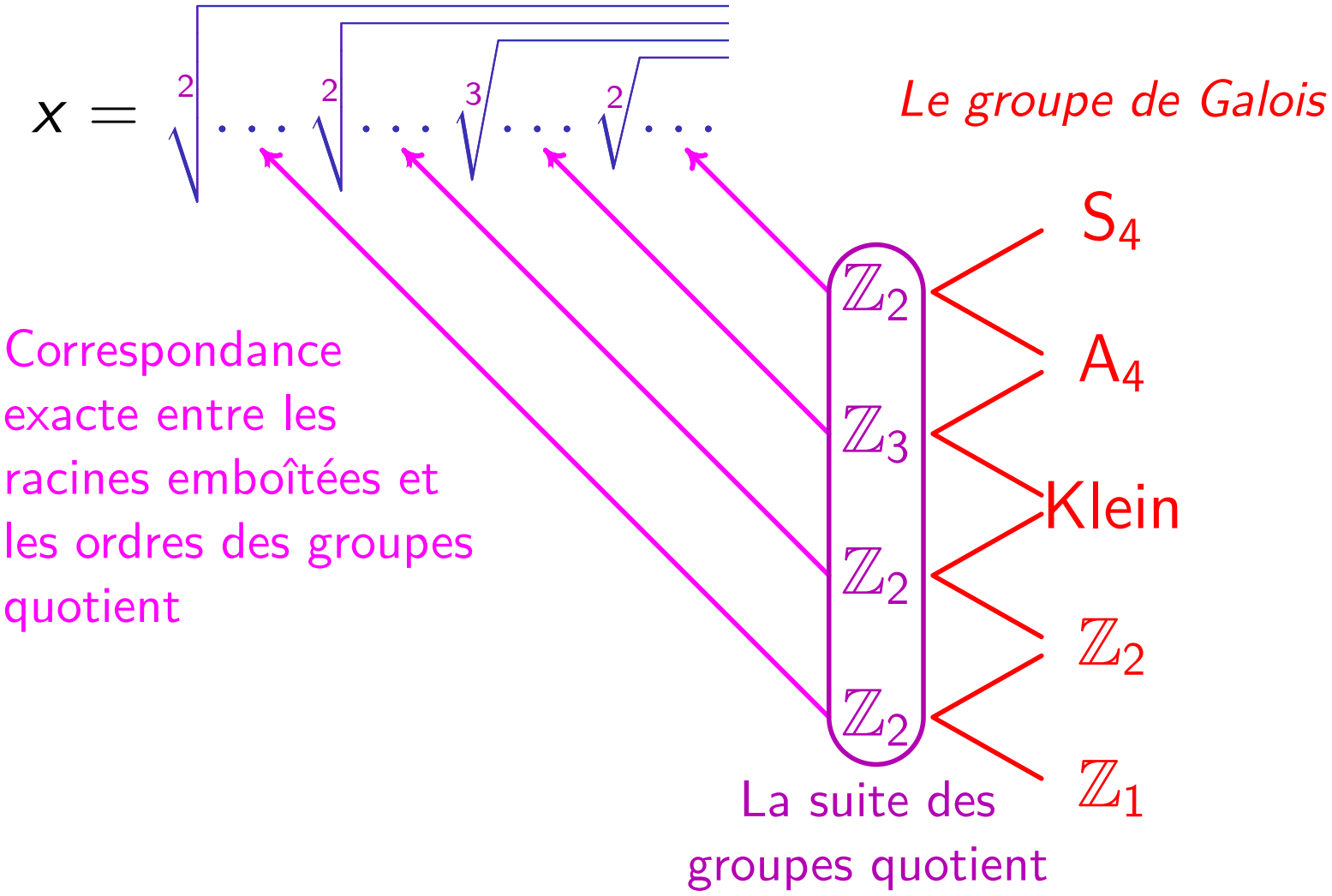
S_4 — groupe résoluble ! ! !

Équation quartique — résoluble par radicaux ! ! !

S_4	24 éléments	$S_4/A_4 \sim$	$\mathbb{Z}_2$
A_4	12 éléments	$A_4/\text{Klein} \sim$	$\mathbb{Z}_3$
Klein	4 éléments	$\text{Klein}/\mathbb{Z}_2 \sim$	$\mathbb{Z}_2$
$\mathbb{Z}_2$	2 éléments	$\mathbb{Z}_2/\mathbb{Z}_1 \sim$	$\mathbb{Z}_2$
$\mathbb{Z}_1$	1 élément		

La formule de résolution de la quartique générale

$$x^4 + bx^3 + cx^2 + dx + e = 0$$



Pour l'équation *quintique* la plus générale, il y a symétrie totale des 5 racines — donc S_5 avec $120 = 5\,!$ éléments.
C'est le groupe des symétries de l'icosaèdre (rotations et réflexions).

S_5 — groupe NON résoluble ! ! !

Équation quintique — NON résoluble par radicaux ! ! !

S_5 — 120 éléments

$S_5/A_5 \sim \mathbb{Z}_2$

A_5 — 60 éléments

? ? ? ?

Rien ! A_5 est un groupe *simple* ; aucun sous-groupe distingué !

$\mathbb{Z}_1$

←

Alors nous voyons que les clés les plus simples n'ouvrent pas toutes les portes.

C'est ça, l'apport de Galois ?

Mais non !

←

Les idées d'Évariste Galois vont très très loin au-delà de la non résolubilité des équations polynomiales.

- La théorie des groupes abstraits
- La théorie des corps
- La théorie des treillis des structures abstraites et de leurs sous-structures
- La théorie des correspondances entre les treillis

(« théorie de Galois »)

←

Et les mathématiciens modernes, inspirés par Galois, ont généralisé toutes ces idées à maintes reprises, trouvant partout groupes, treillis, et isomorphies cachées.

Voilà le vrai apport d'Évariste Galois, 180 ans plus tard.

Quel radical !

←

Quitter