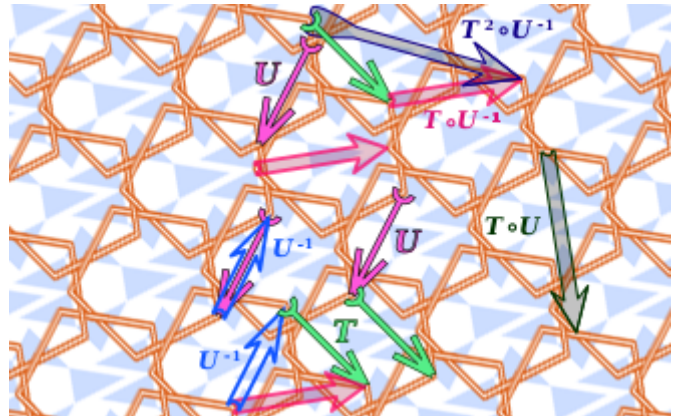


Invariant (mathematics)

In mathematics, an **invariant** is a property, held by a class of mathematical objects, which remains unchanged when transformations of a certain type are applied to the objects. The particular class of objects and type of transformations are usually indicated by the context in which the term is used. For example, the area of a triangle is an invariant with respect to isometries of the Euclidean plane. The phrases "invariant under" and "invariant to" a transformation are both used. More generally, an invariant with respect to an equivalence relation is a property that is constant on each equivalence class.

Invariants are used in diverse areas of mathematics such as geometry, topology, algebra and discrete mathematics. Some important classes of transformations are defined by an invariant they leave unchanged, for example conformal maps are defined as transformations of the plane that preserve angles. The discovery of invariants is an important step in the process of classifying mathematical objects.



A wallpaper is **invariant** under an infinite number of translations, members of a group, of which the operation denoted by \circ is the function composition.

Contents

Examples

MU puzzle

Invariant set

Formal statement

Unchanged under group action

Independent of presentation

Unchanged under perturbation

Invariants in computer science

Automatic invariant detection in imperative programs

See also

Notes

References

External links

Examples

A simple example of invariance is expressed in our ability to count. For a finite set of objects of any kind, there is a number to which we always arrive, regardless of the order in which we count the objects in the set. The quantity—a cardinal number—is associated with the set, and is invariant under the process of counting.

An identity is an equation that remains true for all values of its variables. There are also inequalities that remain true when the values of their variables change.

The distance between two points on a number line is not changed by adding the same quantity to both numbers. On the other hand, multiplication does not have this same property as addition, so distance is not invariant under multiplication.

Angles and ratios of distances are invariant under scalings, rotations, translations and reflections. These transformations produce similar shapes, which is the basis of trigonometry. In contrast, angles and ratios are not invariant under non-uniform scaling (such as stretching). The sum of a triangle's interior angles (180°) is invariant under all the above operations. As another example, all circles are similar: they can be transformed into each other and the ratio of the circumference to the diameter is invariant (denoted by the Greek letter π).

Some more complicated examples:

- The real part and the absolute value of a complex number are invariant under complex conjugation.
- The degree of a polynomial is invariant under linear change of variables.
- The dimension and homology groups of a topological object are invariant under homeomorphism.^[1]
- The number of fixed points of a dynamical system is invariant under many mathematical operations.
- Euclidean distance is invariant under orthogonal transformations.
- Euclidean area is invariant under a linear map with determinant 1 (see Equi-area maps).
- Some invariants of projective transformations: collinearity of three or more points, concurrency of three or more lines, conic sections, the cross-ratio.^[2]
- The determinant, trace, and eigenvectors and eigenvalues of a square matrix are invariant under changes of basis. In a word, the spectrum of a matrix is invariant to the change of basis.
- Invariants of tensors.
- The singular values of a matrix are invariant under orthogonal transformations.
- Lebesgue measure is invariant under translations.
- The variance of a probability distribution is invariant under translations of the real line; hence the variance of a random variable is unchanged by the addition of a constant to it.
- The fixed points of a transformation are the elements in the domain invariant under the transformation. They may, depending on the application, be called symmetric with respect to that transformation. For example, objects with translational symmetry are invariant under certain translations.
- The integral $\int_M K d\mu$ of the Gaussian curvature K of a 2-dimensional Riemannian manifold (M, g) is invariant under changes of the Riemannian metric g . This is the Gauss–Bonnet theorem.
- Differential invariants for differential equations.^[3]

MU puzzle

The MU puzzle^[4] is a good example of a logical problem where determining an invariant is of use for an impossibility proof. The puzzle asks one to start with the word MI and transform it into the word MU using in each step one of the following transformation rules:

1. If a string ends with an I, a U may be appended ($xI \rightarrow xIU$)
2. The string after the M may be completely duplicated ($Mx \rightarrow Mxx$)
3. Any three consecutive I's (III) may be replaced with a single U ($xIIIy \rightarrow xUy$)
4. Any two consecutive U's may be removed ($xUUy \rightarrow xy$)

An example derivation (superscripts indicating the applied rules) is

$$MI \xrightarrow{2} MII \xrightarrow{2} MIII \xrightarrow{3} MUI \xrightarrow{2} MUIUI \xrightarrow{1} MUIUIU \xrightarrow{2} MUIUIUIUIU \xrightarrow{4} MUIUIUIU \rightarrow \dots$$

Is it possible to convert MI into MU using these four transformation rules only?

One could spend many hours applying these transformation rules to strings. However, it might be quicker to find a property that is invariant to all rules (i.e. that isn't changed by any of them), and demonstrates that getting to MU is impossible. Logically looking at the puzzle, the only way to get rid of any I's is to have three consecutive I's in the string. This makes the following invariant interesting to consider:

The number of I's in the string is not a multiple of 3.

This is an invariant to the problem if for each of the transformation rules the following holds: if the invariant held before applying the rule, it will also hold after applying it. If we look at the net effect of applying the rules on the number of I's and U's we can see this actually is the case for all rules:

Rule	#I's	#U's	Effect on invariant
1	+0	+1	Number of I's is unchanged. If the invariant held, it still does.
2	×2	×2	If n is not a multiple of 3, then $2\times n$ isn't either. The invariant still holds.
3	−3	+1	If n is not a multiple of 3, $n-3$ isn't either. The invariant still holds.
4	+0	−2	Number of I's is unchanged. If the invariant held, it still does.

The table above shows clearly that the invariant holds for each of the possible transformation rules, which basically means that whichever rule we pick, at whatever state, if the number of I's was not a multiple of three before applying the rule, it won't be afterwards either.

Given that there is a single I in the starting string MI, and one is not a multiple of three, it's impossible to go from MI to MU as zero is a multiple of three.

Invariant set

A subset S of the domain U of a mapping $T: U \rightarrow U$ is an **invariant set** under the mapping when $x \in S \Rightarrow T(x) \in S$. Note that the elements of S are not fixed, but rather the set S is fixed in the power set of U . (Some authors use the terminology *setwise invariant*^[5] vs. *pointwise invariant*^[6] to distinguish between these cases.) For example, a circle is an invariant subset of the plane under a rotation about the circle's center. Further, a conical surface is invariant as a set under a homothety of space.

An invariant set of an operation T is also said to be **stable under T** . For example, the normal subgroups that are so important in group theory are those subgroups that are stable under the inner automorphisms of the ambient group.^{[7][8][9]} Other examples occur in linear algebra. Suppose a linear transformation T has an eigenvector \mathbf{v} . Then the line through $\mathbf{0}$ and \mathbf{v} is an invariant set under T . The eigenvectors span an invariant subspace which is stable under T .

When T is a screw displacement, the screw axis is an invariant line, though if the pitch is non-zero, T has no fixed points.

Formal statement

The notion of invariance is formalized in three different ways in mathematics: via group actions, presentations, and deformation.

Unchanged under group action

Firstly, if one has a group G acting on a mathematical object (or set of objects) X , then one may ask which points x are unchanged, "invariant" under the group action, or under an element g of the group.

Very frequently one will have a group acting on a set X and ask which objects in an *associated* set $F(X)$ are invariant. For example, rotation in the plane about a point leaves the point about which it rotates invariant, while translation in the plane does not leave any points invariant, but does leave all lines parallel to the direction of translation invariant as lines. Formally, define the set of lines in the plane P as $L(P)$; then a rigid motion of the plane takes lines to lines – the group of rigid motions acts on the set of lines – and one may ask which lines are unchanged by an action.

More importantly, one may define a *function* on a set, such as "radius of a circle in the plane" and then ask if this function is invariant under a group action, such as rigid motions.

Dual to the notion of invariants are *coinvariants*, also known as *orbits*, which formalizes the notion of *congruence*: objects which can be taken to each other by a group action. For example, under the group of rigid motions of the plane, the perimeter of a triangle is an invariant, while the set of triangles congruent to a given triangle is a coinvariant.

These are connected as follows: invariants are constant on coinvariants (for example, congruent triangles have the same perimeter), while two objects which agree in the value of one invariant may or may not be congruent (two triangles with the same perimeter need not be congruent). In *classification problems*, one seeks to find a *complete set of invariants*, such that if two objects have the same values for this set of invariants, they are congruent.

For example, triangles such that all three sides are equal are congruent under rigid motions, via *SSS congruence*, and thus the lengths of all three sides form a complete set of invariants for triangles. The three angle measures of a triangle are also invariant under rigid motions, but do not form a complete set as incongruent triangles can share the same angle measures. However, if one allows scaling in addition to rigid motions, then the *AAA similarity criterion* shows that this is a complete set of invariants.

Independent of presentation

Secondly, a function may be defined in terms of some presentation or decomposition of a mathematical object; for instance, the *Euler characteristic* of a *cell complex* is defined as the alternating sum of the number of cells in each dimension. One may forget the cell complex structure and look only at the underlying topological space (the manifold) – as different cell complexes give the same underlying manifold, one may ask if the function is *independent* of choice of *presentation*, in which case it is an *intrinsically* defined invariant. This is the case for the Euler characteristic, and a general method for defining and computing invariants is to define them for a given presentation and then show that they are independent of the choice of presentation. Note that there is no notion of a group action in this sense.

The most common examples are:

- The *presentation of a manifold* in terms of coordinate charts – invariants must be unchanged under *change of coordinates*.
- Various *manifold decompositions*, as discussed for Euler characteristic.
- Invariants of a *presentation of a group*.

Unchanged under perturbation

Thirdly, if one is studying an object which varies in a family, as is common in *algebraic geometry* and *differential geometry*, one may ask if the property is unchanged under perturbation – if an object is constant on families or invariant under change of metric, for instance.

Invariants in computer science

In *computer science*, one can encounter invariants that can be relied upon to be true during the execution of a program, or during some portion of it. **It is a logical assertion that is always held to be true during a certain phase of execution.** For example, a *loop invariant* is a condition that is true at the beginning and end of every execution of a loop.

Invariants are especially useful when reasoning about whether a computer program is correct. The theory of *optimizing compilers*, the methodology of *design by contract*, and *formal methods* for determining *program correctness*, all rely heavily on invariants.

Programmers often use assertions in their code to make invariants explicit. Some object oriented programming languages have a special syntax for specifying class invariants.

Automatic invariant detection in imperative programs

Abstract interpretation tools can compute simple invariants of given imperative computer programs. The kind of properties that can be found depend on the abstract domains used. Typical example properties are single integer variable ranges like $0 \leq x < 1024$, relations between several variables like $0 \leq i - j < 2 \cdot n - 1$, and modulus information like $y \% 4 == 0$. Academic research prototypes also consider simple properties of pointer structures.^[10]

More sophisticated invariants generally have to be provided manually. In particular, when verifying an imperative program using the Hoare calculus,^[11] a loop invariant has to be provided manually for each loop in the program, which is one of the reasons this is generally impractical for most programs.

In the context of the above MU puzzle example, there is currently no general automated tool that can detect that a derivation, "MI $\rightarrow \dots \rightarrow$ MU", is impossible only from rules 1-4. However, once the abstraction from the string to the number of its "I"s has been made by hand, leading e.g. to the following C program, an abstract interpretation tool will be able to detect that `ICount%3` can't be 0 and hence the "while"-loop will never terminate.

```
void MUPuzzle(void) {
    volatile int RandomRule;
    int ICount=1, UCount=0;
    while (ICount%3!=0)                // non-terminating loop
        switch(RandomRule) {
            case 1:      UCount+=1; break;
            case 2:      ICount*=2; UCount*=2; break;
            case 3:      ICount-=3;  UCount+=1; break;
            case 4:      UCount-=2;  break;
        }
    }
    // computed invariant: ICount%3==1 || ICount%3==2
}
```

See also

- Erlangen program
- Invariant (physics)
- Invariant estimator in statistics
- Invariant theory
- Invariants of tensors
- Symmetry in mathematics
- Topological invariant
- Invariant differential operator
- Invariant measure
- Mathematical constant
- Mathematical constants and functions

Notes

1. Fraleigh (1976), pp. 166–167)
2. Kay (1969), pp. 219)
3. Differential Invariants for Differential Equations by André Platzer (<http://symbolaris.com/logic/diffinv.html>)
4. Hofstadter, Douglas R. (1999) [1979], *Gödel, Escher, Bach: An Eternal Golden Braid*, Basic Books, ISBN 0-465-02656-7 Here: Chapter I.
5. Barry Simon. *Representations of Finite and Compact Groups*. American Mathematical Soc. p. 16. ISBN 978-0-8218-7196-6.
6. Judith Cederberg (1989). *A Course in Modern Geometries*. Springer. p. 174. ISBN 978-1-4757-3831-5.
7. Fraleigh (1976), p. 103)
8. Herstein (1964), p. 42)
9. McCoy (1968), p. 183)

10. Bouajjani, A.; Drăgoi, C.; Enea, C.; Rezie, A.; Sighireanu, M. (2010). "Invariant Synthesis for Programs Manipulating Lists with Unbounded Data". *Proc. CAV*.
11. Hoare, C. A. R. (October 1969). "An axiomatic basis for computer programming" (<https://web.archive.org/web/20160304013345/http://www.spatial.maine.edu/~worboys/processes/hoare%20axiomatic.pdf>) (PDF). *Communications of the ACM*. **12** (10): 576–580. doi:10.1145/363235.363259 (<https://doi.org/10.1145%2F363235.363259>). Archived from the original (<http://www.spatial.maine.edu/~worboys/processes/hoare%20axiomatic.pdf>) (PDF) on 2016-03-04.

References

- Fraleigh, John B. (1976), *A First Course In Abstract Algebra* (2nd ed.), Reading: Addison-Wesley, ISBN 0-201-01984-1
- Herstein, I. N. (1964), *Topics In Algebra*, Waltham: Blaisdell Publishing Company, ISBN 978-1114541016
- Kay, David C. (1969), *College Geometry*, New York: Holt, Rinehart and Winston, LCCN 69-12075 (<https://lccn.loc.gov/69-12075>)
- McCoy, Neal H. (1968), *Introduction To Modern Algebra, Revised Edition*, Boston: Allyn and Bacon, LCCN 68-15225 (<https://lccn.loc.gov/68-15225>)
- J.D. Fokker, H. Zantema, S.D. Swierstra (1991). "Iteratie en invariatie", Programmeren en Correctheid. Academic Service. ISBN 90-6233-681-7.
- Weisstein, Eric W. "Invariant" (<http://mathworld.wolfram.com/Invariant.html>). *MathWorld*.
- Popov, V.L. (2001) [1994], "Invariant" (<https://www.encyclopediaofmath.org/index.php?title=I/i052200>), in Hazewinkel, Michiel (ed.), *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4

External links

- "Applet: Visual Invariants in Sorting Algorithms" (<http://www.u.arizona.edu/~wbraynen/software/VisualInvariants/index.html>) by William Braynen in 1997

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Invariant_\(mathematics\)&oldid=900315526](https://en.wikipedia.org/w/index.php?title=Invariant_(mathematics)&oldid=900315526)"

This page was last edited on 4 June 2019, at 20:48 (UTC).

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.