GF(2)

From Wikipedia, the free encyclopedia

GF(2) (also $\mathbf{F}_2$, $\mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}_2$) is the **G**alois **f**ield of two elements. It is the smallest finite field.

Contents

Definition

The two elements are nearly always called 0 and 1, being the additive and multiplicative identities, respectively.

The field's addition operation is given by the table below, which corresponds to the logical XOR operation.

+	**0**	**1**
0	0	1
1	1	0

The field's multiplication operation corresponds to the logical AND operation.

×	**0**	**1**
0	0	0
1	0	1

One may also define GF(2) as the quotient ring of the ring of integers $\mathbf{Z}$ by the ideal $2\mathbf{Z}$ of all even numbers: GF(2) = $\mathbf{Z}/2\mathbf{Z}$.

Properties

Main article: finite field

Because GF(2) is a field, many of the familiar properties of number systems such as the rational numbers and real numbers are retained:

- addition has an identity element (0) and an inverse for every element;
- multiplication has an identity element (1) and an inverse for every element but 0;
- addition and multiplication are commutative and associative;

- multiplication is distributive over addition.

Properties that are not familiar from the real numbers include:

- every element x of GF(2) satisfies $x+x=0$ and therefore $-x = x$;
- every element x of GF(2) satisfies $x^2 = x$.

Applications

Because of the algebraic properties above, many familiar and powerful tools of mathematics work in GF(2) just as well as other fields. For example, matrix operations, including matrix inversion, can be applied to matrices with elements in GF(2) (*see* matrix ring).

Any abelian group V with the property $v+v=0$ for every v in V can be turned into a vector space over GF(2) in a natural fashion, by defining $0v= 0$ and $1v=v$. This vector space will have a basis, implying that the number of elements of V must be a power of 2 (or infinite).

Since modern computers represent data with binary code, a field with two elements, GF(2), is an important tool for studying algorithms on these machines. GF(2) can be extended to arbitrarily large fields GF(2^n), allowing definition of bitwise operations on strings of bits. Properties of LFSRs, checksums and some ciphers can be studied in this way.

References

- Lidl, Rudolf; Niederreiter, Harald (1997). *Finite fields*. Encyclopedia of Mathematics and Its Applications **20** (2nd ed.). Cambridge University Press. ISBN 0-521-39231-4. Zbl 0866.11069 (http://www.zentralblatt-math.org/zmath/en/search/?format=complete&q=an:0866.11069).

Retrieved from "http://en.wikipedia.org/w/index.php?title=GF(2)&oldid=536646729"
Categories: Finite fields

- This page was last modified on 5 February 2013 at 05:49.
- 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.