ZENODO. 10.5281/zenodo.1252422

The group of the Fermat Numbers

Amelia Carolina Sparavigna
Department of Applied Science and Technology, Politecnico di Torino, Torino, Italy

Abstract: In this work we are discussing the group that we can obtain if we consider the Fermat numbers with a generalized sum.

Keywords: generalized sum, groups, Abelian groups, transcendental functions, logarithmic and exponential functions, Fermat numbers.

Turin, 24 May 2018. DOI: 10.5281/zenodo.1252422

In [1] we find that there are two definitions of the Fermat numbers. We have a less common definition giving a Fermat number as $F_n = 2^n + 1$, which is obtained by setting *x*=1 in a Fermat polynomial of *x*, and the commonly encounter definition $F_n = 2^{2^n} + 1$, which is a subset of the previous assembly of numbers. Here we will consider numbers $F_n = 2^n + 1$ and - as we have recently proposed in [2] for q-integers and Mersenne numbers - investigate the set of them to find its generalized sum which defines the operation of the group.

Let us remember that a group is a set *A* having an operation • which is combining the elements of *A*. That is, the operation combines any two elements *a,b* to form another element of the group denoted *a•b*. To qualify (*A*,•) as a group, the set and operation must satisfy the following requirements. *Closure***:** For all *a*,*b* in *A*, the result of the operation *a•b* is also in *A*. *Associativity:* For all *a*,*b* and *c* in *A,* it holds (*a•b*)•*c* = *a*•(*b•c*). *Identity element*: An element *e* exists in *A*, such that for all elements *a* in *A*, it is *e•a* = *a•e* = *a*. *Inverse element:* For each *a* in *A*, there exists an element *b* in *A* such that *a•b* = *b•a* = *e*, where *e* is the identity (the notation is inherited from the multiplicative operation). A further requirement, is the c*ommutativity:* For all *a*,*b* in *A*, *a•b* = *b•a*. In this case, the group is an Abelian group. For an Abelian group, one may choose to denote the *operation* by + , the *identity element* becomes the *neutral element* and the inverse element the *opposite element*. In this case, the group is called an additive group.

The generalized sum for the Fermat numbers $F_n = 2^n + 1$ is:

$$F_m \oplus F_n = 2 - F_m - F_n + F_m F_n = (1 - F_m) + (1 - F_n) + F_m F_n \quad (1)$$

To have (1), let us evaluate:

$$F_{m+n} = 2^{m+n} + 1 = F_m \oplus F_n = 2 - F_m - F_n + F_m F_n = 2 - (2^m + 1) - (2^n + 1) + (2^m + 1)(2^n + 1)$$

$$2^{m+n} + 1 = 2 - 2^m - 2^n - 2 + 2^m 2^n + 2^n + 2^m + 1$$

This gives also the *closure* of the group.

We can provide a recurrence relation as: $F_{n+1} = 2^{n+1} + 1 = F_n \oplus F_1$

From (1), we can see that the *neutral element* is not 0. We have to use as a *neutral element* the integer 2, which is $F_0 = 2^0 + 1 = 2$ and then an element of the group. We have:

$$F_n \oplus F_0 = 2 - F_n - F_0 + F_n F_0 = F_n$$

The *opposite element* is defined by $F_n \oplus Opposite(F_n) = 2$. We have:

$$Opposite(F_n) = \frac{F_n}{F_n - 1} = 1 + 2^{-n} = F_{-n} \qquad (2)$$

Then, to have a group we need to add numbers (2) to the set of the Fermat numbers.

Therefore, we consider 2 as the *neutral element ,* and the *opposite element* as given by (2).

Let us consider three Fermat numbers F_n , F_m , F_l ; to have a group we need the *associativity* of the generalized sum, so that $(F_m \oplus F_n) \oplus F_l = F_m \oplus (F_n \oplus F_l)$. Let us call $x = F_n$, $y = F_m$, $z = F_l$ and evaluate:

$$(x \oplus y) \oplus z = 2 - (x \oplus y) - z + (x \oplus y) z = 2 - 2 + x + y - xy - z + 2z - xz - yz + xyz$$

$$(x \oplus y) \oplus z = x + y + z - xy - xz - yz + xyz \qquad (3)$$

And:

$$x \oplus (y \oplus z) = 2 - x - (y \oplus z) + x (y \oplus z) = 2 - x - (2 - y - z + yz) + x (2 - y - z + yz)$$

$$x \oplus (y \oplus z) = x + y + z - xy - xz - yz + xyz \qquad (4)$$

From (3) and (4), we have the *associativity*. The *commutativity* is evident.

We have already considered the generalized sum (1) in a recent work [3].

In [3], we consider some functions $G(x)$, having inverses so that $G^{-1}(G(x))=x$, which are *generators* of *group law* [4-6]:

$$\Phi(x,y)=G(G^{-1}(x)+G^{-1}(y))$$

The *group law* is giving the *generalized sum* of the group $x\oplus y=G(G^{-1}(x)+G^{-1}(y))$.

In [3] we considered the following generator and inverse:

$$G(x)=\mathrm{e}^{-2x}(\mathrm{e}^{2x}+1) \qquad G^{-1}(x)=\ln(\frac{1}{\sqrt{x-1}}) \quad (5)$$

and investigate a possible group from them. The *group law* $\Phi(x,y)$ gives the generalized sum:

$$x\oplus y=G(G^{-1}(x)+G^{-1}(y))=G(\ln(\frac{1}{\sqrt{x-1}})+\ln(\frac{1}{\sqrt{y-1}}))=G(\ln(\frac{1}{\sqrt{x-1}}\frac{1}{\sqrt{y-1}}))=G(\ln\frac{1}{Z})$$

$$G(\ln\frac{1}{Z})=\mathrm{e}^{-2\ln Z}(e^{2\ln Z}+1)=(x-1)(y-1)(\frac{1}{(x-1)(y-1)}+1)$$

$$x\oplus y=2-x-y+xy=(1-x)+(1-y)+xy \qquad (6)$$

And (6) is the generalized sum (1) proposed for the Fermat numbers.

Let us also note that, if we use (5), we need $x>1$. And this is a condition satisfied by the Fermat numbers and their opposites (2).

References

1. Weisstein, Eric W. "Fermat Number." From MathWorld--A Wolfram Web Resource. http://mathworld.wolfram.com/FermatNumber.html

2. Sparavigna, A. C. (2018). The q-integers and the Mersenne numbers. Zenodo. DOI: 10.5281/zenodo.1251833

3. Sparavigna, A. C. (2018). Generalized Sums Based on Transcendental Functions. Zenodo. DOI: 10.5281/zenodo.1250020

4. Sicuro, G., & Tempesta, P. (2016). Groups, information theory, and Einstein's likelihood principle. Phys. Rev. E 93, 040101(R).

5. Curado, E. M., Tempesta, P., & Tsallis, C. (2016). A new entropy based on a group-theoretical structure. Annals of Physics, 366, 22-31.