WIKIPEDIA

Field norm

In mathematics, the **(field) norm** is a particular mapping defined in field theory, which maps elements of a larger field into a subfield.

Contents

Formal definition

Let K be a field and L a finite extension (and hence an algebraic extension) of K. The field L is then a finite dimensional vector space over K. Multiplication by α, an element of L,

$$m_\alpha : L \to L \text{ given by } m_\alpha(x) = \alpha x,$$

is a K-linear transformation of this vector space into itself. The *norm*, $\mathbf{N}_{L/K}(\alpha)$, is defined as the determinant of this linear transformation.[1]

For nonzero α in L, let $\sigma_1(\alpha)$, ..., $\sigma_n(\alpha)$ be the roots (counted with multiplicity) of the minimal polynomial of α over K (in some extension field of L), then

$$\mathrm{N}_{L/K}(\alpha) = \left(\prod_{j=1}^{n} \sigma_j(\alpha)\right)^{[L:K(\alpha)]}.$$

If L/K is separable then each root appears only once in the product (the exponent $[L:K(\alpha)]$ may still be greater than 1).

More particularly, if L/K is a Galois extension and α is in L, then the norm of α is the product of all the Galois conjugates of α, i.e.

$$\mathrm{N}_{L/K}(\alpha) = \prod_{g \in \mathrm{Gal}(L/K)} g(\alpha),$$

where Gal(L/K) denotes the Galois group of L/K.[2]

Example

The field norm from the complex numbers to the real numbers sends

$$x + iy$$

to

$$x^2 + y^2,$$

because the Galois group of $\mathbb{C}$ over $\mathbb{R}$ has two elements, the identity element and complex conjugation, and taking the product yields $(x + iy)(x - iy) = x^2 + y^2$.

In this example the norm was the square of the usual Euclidean distance norm in $\mathbb{C}$. In general, the field norm is very different from the usual distance norm. We will illustrate that with an example where the field norm can be negative. Consider the number field $K = \mathbb{Q}(\sqrt{2})$. The Galois group of K over $\mathbb{Q}$ has order $d = 2$ and is generated by the element which sends $\sqrt{2}$ to $-\sqrt{2}$. So the norm of $1 + \sqrt{2}$ is:

$$(1 + \sqrt{2})(1 - \sqrt{2}) = -1.$$

The field norm can also be obtained without the Galois group. Fix a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$, say $\{1, \sqrt{2}\}$: then multiplication by the number $1 + \sqrt{2}$ sends 1 to $1 + \sqrt{2}$ and $\sqrt{2}$ to $2 + \sqrt{2}$. So the determinant of "multiplying by $1 + \sqrt{2}$ is the determinant of the matrix which sends the vector $(1, 0)^{\mathrm{T}}$ (corresponding to the first basis element, i.e. 1) to $(1, 1)^{\mathrm{T}}$ and the vector $(0, 1)^{\mathrm{T}}$ (which represents the second basis element $\sqrt{2}$) to $(2, 1)^{\mathrm{T}}$, viz.:

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}.$$

The determinant of this matrix is −1.

Properties of the norm

Several properties of the norm function hold for any finite extension.[3]

The norm $\mathbf{N}_{L/K} : L^* \to K^*$ is a group homomorphism from the multiplicative group of L to the multiplicative group of K, that is

$$\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta) \text{ for all } \alpha, \beta \in L^* .$$

Furthermore, if a in K:

$$\mathrm{N}_{L/K}(a\alpha) = a^{[L:K]}\,\mathrm{N}_{L/K}(\alpha) \text{ for all } \alpha \in L.$$

If $a \in K$ then $\mathrm{N}_{L/K}(a) = a^{[L:K]}$.

Additionally, the norm behaves well in towers of fields: if *M* is a finite extension of *L*, then the norm from *M* to *K* is just the composition of the norm from *M* to *L* with the norm from *L* to *K*, i.e.

$$\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}.$$

Finite fields

Let $L = \mathrm{GF}(q^n)$ be a finite extension of a finite field $K = \mathrm{GF}(q)$. Since L/K is a Galois extension, if α is in *L*, then the norm of α is the product of all the Galois conjugates of α, i.e.[4]

$$\mathrm{N}_{L/K}(\alpha) = \alpha \bullet \alpha^q \bullet \cdots \bullet \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}.$$

In this setting we have the additional properties,[5]

- $\mathrm{N}_{L/K}(\alpha^q) = \mathrm{N}_{L/K}(\alpha)$ for all $\alpha \in L$
- for any $a \in K,$ we have $\mathrm{N}_{L/K}(a) = a^n$.

Further properties

The norm of an algebraic integer is again an integer, because it is equal (up to sign) to the constant term of the characteristic polynomial.

In algebraic number theory one defines also norms for ideals. This is done in such a way that if I is an ideal of O_K, the ring of integers of the number field K, $\mathbf{N}(I)$ is the number of residue classes in O_K/I – i.e. the cardinality of this finite ring. Hence this **norm of an ideal** is always a positive integer. When I is a principal ideal αO_K then $\mathbf{N}(I)$ is equal to the absolute value of the norm to Q of α, for α an algebraic integer.

See also

- Field trace
- Ideal norm
- Norm form

Notes

1. Rotman 2002, p. 940
2. Rotman 2002, p. 943
3. Roman 1995, p. 151 (1st ed.)
4. Lidl & Niederreiter 1997, p.57
5. Mullen & Panario 2013, p. 21

References

- Lidl, Rudolf; Niederreiter, Harald (1997) [1983], *Finite Fields*, Encyclopedia of Mathematics and its Applications, **20** (Second ed.), Cambridge University Press, ISBN 0-521-39231-4, Zbl 0866.11069 (https://zbmath.org/?format=complete&q=an:0866.11069)
- Mullen, Gary L.; Panario, Daniel (2013), *Handbook of Finite Fields*, CRC Press, ISBN 978-1-4398-7378-6
- Roman, Steven (2006), *Field theory*, Graduate Texts in Mathematics, **158** (Second ed.), Springer, Chapter 8, ISBN 978-0-387-27677-9, Zbl 1172.12001 (https://zbmath.org/?format=complete&q=an:1172.12001)
- Rotman, Joseph J. (2002), *Advanced Modern Algebra*, Prentice Hall, ISBN 978-0-13-087868-7