Frobenius endomorphism

In commutative algebra and field theory, the **Frobenius endomorphism** (after Ferdinand Georg Frobenius) is a special endomorphism of commutative rings with prime characteristic p, an important class which includes finite fields. The endomorphism maps every element to its p-th power. In certain contexts it is an automorphism, but this is not true in general.

Contents

Definition

Let R be a commutative ring with prime characteristic p (an integral domain of positive characteristic always has prime characteristic, for example). The Frobenius endomorphism F is defined by

$$F(r) = r^p$$

for all r in R. It respects the multiplication of R:

$$F(rs) = (rs)^p = r^p s^p = F(r)F(s)\ ,$$

and $F(1)$ is clearly 1 also. What is interesting, however, is that it also respects the addition of R. The expression $(r + s)^p$ can be expanded using the binomial theorem. Because p is prime, it divides $p!$ but not any $q!$ for $q < p$; it therefore will divide the numerator, but not the denominator, of the explicit formula of the binomial coefficients

$$\frac{p!}{k!(p-k)!},$$

if $1 \le \mathrm{k} \le p - 1$. Therefore, the coefficients of all the terms except r^p and s^p are divisible by p, the characteristic, and hence they vanish.[1] Thus

$$F(r+s) = (r+s)^p = r^p + s^p = F(r) + F(s)\ .$$

This shows that F is a ring homomorphism.

If $\varphi : R \to S$ is a homomorphism of rings of characteristic p, then

$$\phi(x^p) = \phi(x)^p.$$

If F_R and F_S are the Frobenius endomorphisms of R and S, then this can be rewritten as:

$$\phi \circ F_R = F_S \circ \phi.$$

This means that the Frobenius endomorphism is a natural transformation from the identity functor on the category of characteristic p rings to itself.

If the ring R is a ring with no nilpotent elements, then the Frobenius endomorphism is injective: $F(r) = 0$ means $r^p = 0$, which by definition means that r is nilpotent of order at most p. In fact, this is an if and only if, because if r is any nilpotent, then one of its powers will be nilpotent of order at most p. In particular, if R is a field then the Frobenius endomorphism is injective.

The Frobenius morphism is not necessarily surjective, even when R is a field. For example, let $K = \mathbf{F}_p(t)$ be the finite field of p elements together with a single transcendental element; equivalently, K is the field of rational functions with coefficients in $\mathbf{F}_p$. Then the image of F does not contain t. If it did, then there would be a rational function $q(t)/r(t)$ whose p-th power $q(t)^p/r(t)^p$ would equal t. But the degree of this p-th power is $p \deg(q) - p \deg(r)$, which is a multiple of p. In particular, it can't be 1, which is the degree of t. This is a contradiction; so t is not in the image of F.

A field K is called *perfect* if either it is of characteristic zero or it is of positive characteristic and its Frobenius endomorphism is an automorphism. For example, all finite fields are perfect.

Fixed points of the Frobenius endomorphism

Consider the finite field $\mathbf{F}_p$. By Fermat's little theorem, every element x of $\mathbf{F}_p$ satisfies $x^p = x$. Equivalently, it is a root of the polynomial $X^p - X$. The elements of $\mathbf{F}_p$ therefore determine p roots of this equation, and because this equation has degree p it has no more than p roots over any extension. In particular, if K is an algebraic extension of $\mathbf{F}_p$ (such as the algebraic closure or another finite field), then $\mathbf{F}_p$ is the fixed field of the Frobenius automorphism of K.

Let R be a ring of characteristic $p > 0$. If R is an integral domain, then by the same reasoning, the fixed points of Frobenius are the elements of the prime field. However, if R is not a domain, then $X^p - X$ may have more than p roots; for example, this happens if $R = \mathbf{F}_p \times \mathbf{F}_p$.

A similar property is enjoyed on the finite field $\mathbf{F}_{p^e}$ by the eth iterate of the Frobenius automorphism: Every element of $\mathbf{F}_{p^e}$ is a root of $X^{p^e} - X$, so if K is an algebraic extension of $\mathbf{F}_{p^e}$ and F is the Frobenius automorphism of K, then the fixed field of F^e is $\mathbf{F}_{p^e}$. If R is a domain which is an $\mathbf{F}_{p^e}$-algebra, then the fixed points of the eth iterate of Frobenius are the elements of the image of $\mathbf{F}_{p^e}$.

Iterating the Frobenius map gives a sequence of elements in R:

$$x, x^p, x^{p^2}, x^{p^3}, \ldots.$$

This sequence of iterates is used in defining the Frobenius closure and the tight closure of an ideal.

As a generator of Galois groups

The Galois group of an extension of finite fields is generated by an iterate of the Frobenius automorphism. First, consider the case where the ground field is the prime field. Let $\mathbf{F}_q$ be the finite field of q elements, where $q = p^e$. The Frobenius automorphism F of $\mathbf{F}_q$ fixes the prime field $\mathbf{F}_p$, so it is an element of the Galois group $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$. In fact, since $\mathbf{F}_q{}^\times$ is cyclic with $q - 1$ elements,

we know that the Galois group is cyclic and F is a generator. The order of F is e because F^e acts on an element x by sending it to x^q, and this is the identity on elements of $\mathbf{F}_q$. Every automorphism of $\mathbf{F}_q$ is a power of F, and the generators are the powers F^i with i coprime to e.

Now consider the finite field $\mathbf{F}_{q^f}$ as an extension of $\mathbf{F}_q$. The Frobenius automorphism F of $\mathbf{F}_{q^f}$ does not fix the ground field $\mathbf{F}_q$, but its e-th iterate F^e does. The Galois group $\mathrm{Gal}(\mathbf{F}_{q^f}/\mathbf{F}_q)$ is cyclic of order f and is generated by F^e. It is the subgroup of $\mathrm{Gal}(\mathbf{F}_{q^f}/\mathbf{F}_p)$ generated by F^e. The generators of $\mathrm{Gal}(\mathbf{F}_{q^f}/\mathbf{F}_q)$ are the powers F^{ei} where i is coprime to f.

The Frobenius automorphism is not a generator of the absolute Galois group

$$\mathrm{Gal}\left(\overline{\mathbf{F}_q}/\mathbf{F}_q\right),$$

because this Galois group is

$$\widehat{\mathbf{Z}} = \varprojlim_n \mathbf{Z}/n\mathbf{Z},$$

which is not cyclic. However, because the Frobenius automorphism is a generator of the Galois group of every finite extension of $\mathbf{F}_q$, it is a generator of every finite quotient of the absolute Galois group. Consequently, it is a topological generator in the usual Krull topology on the absolute Galois group.

Frobenius for schemes

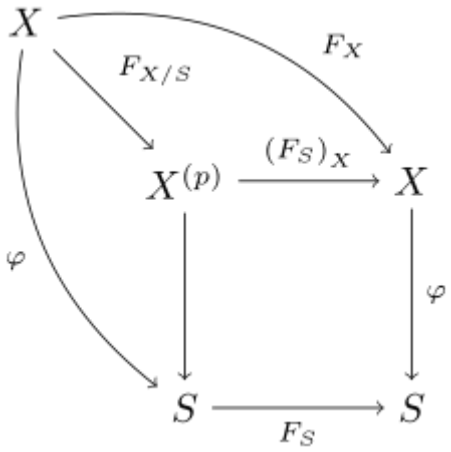
There are several different ways to define the Frobenius morphism for a scheme. The most fundamental is the absolute Frobenius morphism. However, the absolute Frobenius morphism behaves poorly in the relative situation because it pays no attention to the base scheme. There are several different ways of adapting the Frobenius morphism to the relative situation, each of which is useful in certain situations.

The absolute Frobenius morphism

Suppose that X is a scheme of characteristic $p > 0$. Choose an open affine subset $U = \mathrm{Spec}\ A$ of X. The ring A is an $\mathbf{F}_p$-algebra, so it admits a Frobenius endomorphism. If V is an open affine subset of U, then by the naturality of Frobenius, the Frobenius morphism on U, when restricted to V, is the Frobenius morphism on V. Consequently, the Frobenius morphism glues to give an endomorphism of X. This endomorphism is called the **absolute Frobenius morphism** of X. By definition, it is a homeomorphism of X with itself. The absolute Frobenius morphism is a natural transformation from the identity functor on the category of $\mathbf{F}_p$-schemes to itself.

If X is an S-scheme and the Frobenius morphism of S is the identity, then the absolute Frobenius morphism is a morphism of S-schemes. In general, however, it is not. For example, consider the ring $A = \mathbf{F}_{p^2}$. Let X and S both equal $\mathrm{Spec}\ A$ with the structure map $X \to S$ being the identity. The Frobenius morphism on A sends a to a^p. It is not a morphism of $\mathbf{F}_{p^2}$-algebras. If it were, then multiplying by an element b in $\mathbf{F}_{p^2}$ would commute with applying the Frobenius endomorphism. But this is not true because:

$$b \cdot a = ba \neq F(b) \cdot a = b^p a.$$



Let $\varphi : X \to S$ be a morphism of schemes, and denote the absolute Frobenius morphisms of S and X by F_S and F_X, respectively. Define $X^{(p)}$ to be the base change of X by F_S. Then the above diagram commutes and the square is Cartesian. The morphism $F_{X/S}$ is relative Frobenius.

The former is the action of b in the $\mathbf{F}_{p^2}$-algebra structure that A begins with, and the latter is the action of $\mathbf{F}_{p^2}$ induced by Frobenius. Consequently the Frobenius morphism on $\operatorname{Spec} A$ is not a morphism of $\mathbf{F}_{p^2}$-schemes.

The absolute Frobenius morphism is a purely inseparable morphism of degree p. Its differential is zero. It preserves products, meaning that for any two schemes X and Y, $F_{X\times Y} = F_X \times F_Y$.

Restriction and extension of scalars by Frobenius

Suppose that $\varphi : X \to S$ is the structure morphism for an S-scheme X. The base scheme S has a Frobenius morphism F_S. Composing φ with F_S results in an S-scheme X_F called the **restriction of scalars by Frobenius**. The restriction of scalars is actually a functor, because an S-morphism $X \to Y$ induces an S-morphism $X_F \to Y_F$.

For example, consider a ring A of characteristic $p > 0$ and a finitely presented algebra over A:

$$R = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m).$$

The action of A on R is given by:

$$c \cdot \sum a_\alpha X^\alpha = \sum c a_\alpha X^\alpha,$$

where α is a multi-index. Let $X = \operatorname{Spec} R$. Then X_F is the affine scheme $\operatorname{Spec} R$, but its structure morphism $\operatorname{Spec} R \to \operatorname{Spec} A$, and hence the action of A on R, is different:

$$c \cdot \sum a_\alpha X^\alpha = \sum F(c) a_\alpha X^\alpha = \sum c^p a_\alpha X^\alpha.$$

Because restriction of scalars by Frobenius is simply composition, many properties of X are inherited by X_F under appropriate hypotheses on the Frobenius morphism. For example, if X and S_F are both finite type, then so is X_F.

The **extension of scalars by Frobenius** is defined to be:

$$X^{(p)} = X \times_S S_F.$$

The projection onto the S factor makes $X^{(p)}$ an S-scheme. If S is not clear from the context, then $X^{(p)}$ is denoted by $X^{(p/S)}$. Like restriction of scalars, extension of scalars is a functor: An S-morphism $X \to Y$ determines an S-morphism $X^{(p)} \to Y^{(p)}$.

As before, consider a ring A and a finitely presented algebra R over A, and again let $X = \operatorname{Spec} R$. Then:

$$X^{(p)} = \operatorname{Spec} R \otimes_A A_F.$$

A global section of $X^{(p)}$ is of the form:

$$\sum_i \left(\sum_\alpha a_{i\alpha} X^\alpha \right) \otimes b_i = \sum_i \sum_\alpha X^\alpha \otimes a_{i\alpha}^p b_i,$$

where α is a multi-index and every $a_{i\alpha}$ and b_i is an element of A. The action of an element c of A on this section is:

$$c \cdot \sum_i \left(\sum_\alpha a_{i\alpha} X^\alpha \right) \otimes b_i = \sum_i \left(\sum_\alpha a_{i\alpha} X^\alpha \right) \otimes b_i c.$$

Consequently, $X^{(p)}$ is isomorphic to:

$$\operatorname{Spec} A[X_1, \ldots, X_n] / \left(f_1^{(p)}, \ldots, f_m^{(p)} \right),$$

where, if:

$$f_j = \sum_\beta f_{j\beta} X^\beta,$$

then:

$$f_j^{(p)} = \sum_\beta f_{j\beta}^p X^\beta.$$

A similar description holds for arbitrary A-algebras R.

Because extension of scalars is base change, it preserves limits and coproducts. This implies in particular that if X has an algebraic structure defined in terms of finite limits (such as being a group scheme), then so does $X^{(p)}$. Furthermore, being a base change means that extension of scalars preserves properties such as being of finite type, finite presentation, separated, flat, and so on.

Extension of scalars is well-behaved with respect to base change: Given a morphism $S' \to S$, there is a natural isomorphism:

$$X^{(p/S)} \times_S S' \cong (X \times_S S')^{(p/S')}.$$

Relative Frobenius

The **relative Frobenius morphism** of an S-scheme X is the morphism:

$$F_{X/S} : X \to X^{(p)}$$

defined by:

$$F_{X/S} = (F_X, 1_S).$$

Because the absolute Frobenius morphism is natural, the relative Frobenius morphism is a morphism of S-schemes.

Consider, for example, the A-algebra:

$$R = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m).$$

We have:

$$R^{(p)} = A[X_1, \ldots, X_n]/(f_1^{(p)}, \ldots, f_m^{(p)}).$$

The relative Frobenius morphism is the homomorphism $R^{(p)} \to R$ defined by:

$$\sum_i \sum_\alpha X^\alpha \otimes a_{i\alpha} \mapsto \sum_i \sum_\alpha a_{i\alpha} X^{p\alpha}.$$

Relative Frobenius is compatible with base change in the sense that, under the natural isomorphism of $X^{(p/S)} \times_S S'$ and $(X \times_S S')^{(p/S')}$, we have:

$$F_{X/S} \times 1_{S'} = F_{X \times_S S'/S'}.$$

Relative Frobenius is a universal homeomorphism. If $X \to S$ is an open immersion, then it is the identity. If $X \to S$ is a closed immersion determined by an ideal sheaf I of O_S, then $X^{(p)}$ is determined by the ideal sheaf I^p and relative Frobenius is the augmentation map $O_S/I^p \to O_S/I$.

X is unramified over S if and only if $F_{X/S}$ is unramified and if and only if $F_{X/S}$ is a monomorphism. X is étale over S if and only if $F_{X/S}$ is étale and if and only if $F_{X/S}$ is an isomorphism.

Arithmetic Frobenius

The **arithmetic Frobenius morphism** of an S-scheme X is a morphism:

$$F^a_{X/S} : X^{(p)} \to X \times_S S \cong X$$

defined by:

$$F^a_{X/S} = 1_X \times F_S.$$

That is, it is the base change of F_S by 1_X.

Again, if:

$$R = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m),$$
$$R^{(p)} = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m) \otimes_A A_F,$$

then the arithmetic Frobenius is the homomorphism:

$$\sum_i \left(\sum_\alpha a_{i\alpha} X^\alpha \right) \otimes b_i \mapsto \sum_i \sum_\alpha a_{i\alpha} b_i^p X^\alpha.$$

If we rewrite $R^{(p)}$ as:

$$R^{(p)} = A[X_1, \ldots, X_n] / \left(f_1^{(p)}, \ldots, f_m^{(p)} \right),$$

then this homomorphism is:

$$\sum a_\alpha X^\alpha \mapsto \sum a_\alpha^p X^\alpha.$$

Geometric Frobenius

Assume that the absolute Frobenius morphism of S is invertible with inverse F_S^{-1}. Let $S_{F^{-1}}$ denote the S-scheme $F_S^{-1} : S \to S$. Then there is an extension of scalars of X by F_S^{-1}:

$$X^{(1/p)} = X \times_S S_{F^{-1}}.$$

If:

$$R = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m),$$

then extending scalars by F_S^{-1} gives:

$$R^{(1/p)} = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m) \otimes_A A_{F^{-1}}.$$

If:

$$f_j = \sum_\beta f_{j\beta} X^\beta,$$

then we write:

$$f_j^{(1/p)} = \sum_\beta f_{j\beta}^{1/p} X^\beta,$$

and then there is an isomorphism:

$$R^{(1/p)} \cong A[X_1, \ldots, X_n]/(f_1^{(1/p)}, \ldots, f_m^{(1/p)}).$$

The **geometric Frobenius morphism** of an S-scheme X is a morphism:

$$F^g_{X/S} : X^{(1/p)} \to X \times_S S \cong X$$

defined by:

$$F^g_{X/S} = 1_X \times F_S^{-1}.$$

It is the base change of F_S^{-1} by 1_X.

Continuing our example of A and R above, geometric Frobenius is defined to be:

$$\sum_i \left(\sum_\alpha a_{i\alpha} X^\alpha \right) \otimes b_i \mapsto \sum_i \sum_\alpha a_{i\alpha} b_i^{1/p} X^\alpha.$$

After rewriting $R^{(1/p)}$ in terms of $\{f_j^{(1/p)}\}$, geometric Frobenius is:

$$\sum a_\alpha X^\alpha \mapsto \sum a_\alpha^{1/p} X^\alpha.$$

Arithmetic and geometric Frobenius as Galois actions

Suppose that the Frobenius morphism of S is an isomorphism. Then it generates a subgroup of the automorphism group of S. If $S = \operatorname{Spec} k$ is the spectrum of a finite field, then its automorphism group is the Galois group of the field over the prime field, and the Frobenius morphism and its inverse are both generators of the automorphism group. In addition, $X^{(p)}$ and $X^{(1/p)}$ may be identified with X. The arithmetic and geometric Frobenius morphisms are then endomorphisms of X, and so they lead to an action of the Galois group of k on X.

Consider the set of K-points $X(K)$. This set comes with a Galois action: Each such point x corresponds to a homomorphism $O_X \to k(x) \cong K$ from the structure sheaf to the residue field at x, and the action of Frobenius on x is the application of the Frobenius morphism to the residue field. This Galois action agrees with the action of arithmetic Frobenius: The composite morphism

$$\mathcal{O}_X \to k(x) \xrightarrow{F} k(x)$$

is the same as the composite morphism:

$$\mathcal{O}_X \xrightarrow{F^*_{X/S}} \mathcal{O}_X \to k(x)$$

by the definition of the arithmetic Frobenius. Consequently, arithmetic Frobenius explicitly exhibits the action of the Galois group on points as an endomorphism of X.

Frobenius for local fields

Given an unramified finite extension L/K of local fields, there is a concept of **Frobenius endomorphism** which induces the Frobenius endomorphism in the corresponding extension of residue fields.[2]

Suppose L/K is an unramified extension of local fields, with ring of integers O_K of K such that the residue field, the integers of K modulo their unique maximal ideal φ, is a finite field of order q, where q is a power of a prime. If Φ is a prime of L lying over φ, that L/K is unramified means by definition that the integers of L modulo Φ, the residue field of L, will be a finite field of order q^f extending the residue field of K where f is the degree of L/K. We may define the Frobenius map for elements of the ring of integers O_L of L as an automorphism s_Φ of L such that

$$s_\Phi(x) \equiv x^q \mod \Phi.$$

Frobenius for global fields

In algebraic number theory, **Frobenius elements** are defined for extensions L/K of global fields that are finite Galois extensions for prime ideals Φ of L that are unramified in L/K. Since the extension is unramified the decomposition group of Φ is the Galois group of the extension of residue fields. The Frobenius element then can be defined for elements of the ring of integers of L as in the local case, by

$$s_\Phi(x) \equiv x^q \mod \Phi,$$

where q is the order of the residue field $O_K/(\Phi \cap O_K)$.

Lifts of the Frobenius are in correspondence with p-derivations.

Examples

The polynomial

$$x^5 - x - 1$$

has discriminant

$$19 \times 151,$$

and so is unramified at the prime 3; it is also irreducible mod 3. Hence adjoining a root ρ of it to the field of 3-adic numbers $\mathbf{Q}_3$ gives an unramified extension $\mathbf{Q}_3(\rho)$ of $\mathbf{Q}_3$. We may find the image of ρ under the Frobenius map by locating the root nearest to ρ^3, which we may do by Newton's method. We obtain an element of the ring of integers $\mathbf{Z}_3[\rho]$ in this way; this is a polynomial of degree four in ρ with coefficients in the 3-adic integers $\mathbf{Z}_3$. Modulo 3^8 this polynomial is

$$\rho^3 + 3(460 + 183\rho - 354\rho^2 - 979\rho^3 - 575\rho^4).$$

This is algebraic over $\mathbf{Q}$ and is the correct global Frobenius image in terms of the embedding of $\mathbf{Q}$ into $\mathbf{Q}_3$; moreover, the coefficients are algebraic and the result can be expressed algebraically. However, they are of degree 120, the order of the Galois group, illustrating the fact that explicit computations are much more easily accomplished if p-adic results will suffice.

If L/K is an abelian extension of global fields, we get a much stronger congruence since it depends only on the prime φ in the base field K. For an example, consider the extension $\mathbf{Q}(\beta)$ of $\mathbf{Q}$ obtained by adjoining a root β satisfying

$$\beta^5 + \beta^4 - 4\beta^3 - 3\beta^2 + 3\beta + 1 = 0$$

to $\mathbf{Q}$. This extension is cyclic of order five, with roots

$$2\cos\tfrac{2\pi n}{11}$$

for integer n. It has roots which are Chebyshev polynomials of β:

$$\beta^2 - 2,\ \beta^3 - 3\beta,\ \beta^5 - 5\beta^3 + 5\beta$$

give the result of the Frobenius map for the primes 2, 3 and 5, and so on for larger primes not equal to 11 or of the form $22n + 1$ (which split). It is immediately apparent how the Frobenius map gives a result equal mod p to the p-th power of the root β.

See also

- Perfect field
- Frobenioid
- Finite field § Frobenius automorphism and Galois theory
- universal homeomorphism

References

1. This is known as the Freshman's dream
2. Fröhlich, A.; Taylor, M.J. (1991). *Algebraic number theory*. Cambridge studies in advanced mathematics **27**. Cambridge University Press p. 144. ISBN 0-521-36664-X. Zbl 0744.11001 (https://zbmath.org/?format=complete&q=an:0744.11001).

- Hazewinkel, Michiel, ed. (2001) [1994], "Frobenius automorphism", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Hazewinkel, Michiel, ed. (2001) [1994], "Frobenius endomorphism", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V / Kluwer Academic Publishers, ISBN 978-1-55608-010-4