有限体について

梅崎直也@unaoya

2020 年 2 月 28 日

体とは結合法則、分配法則、交換法則を満たす四則演算のできる数の集まりをいう。特に重要なのは 0 でない数 x に逆数、つまり $xy = 1$ となる y が存在することで、整数全体の集まりはこの性質を持たない。例えば有理数全体の集まりに通常の四則演算を定めたものは体である。これを $\mathbb{Q}$ で表す。実数全体、複素数全体についても同様であり、これらを $\mathbb{R}, \mathbb{C}$ と表そう。

要素の個数が有限個である体を有限体という。ここでは有限体について調べる。

1 有限体の具体例

まず有限体の具体例をいくつか紹介する。

例 1. $\mathbb{Z}/(3)$ を整数全体を 3 で割ったあまりが等しいものを同一視してできる集合とする。つまり、要素としては $\{[0], [1], [2]\}$ の 3 つからなる有限集合を考える。ここで、$[1]$ というのは 3 で割ったあまりが 1 であることを意味する。つまり、$[1] = [4] = [7] = \cdots$ であり、$[2] = [5] = [8] = \cdots$ であり、$[0] = [3] = [6] = \cdots$ である。このとき、加法と乗法は通常の整数のものを流用して

$$[x] + [y] = [x + y]$$
$$[x][y] = [xy]$$

と定義する。

例えば

$$[1] + [1] = [2]$$
$$[2] + [2] = [4] = [1]$$
$$[1][2] = [2]$$
$$[2][2] = [4] = [1]$$

などと計算できる。

これが結合法則、分配法則、交換法則をみたす。また $[0]$ が加法についての単位元、$[1]$ が乗法についての単位元となる。つまり

$$[0] + [x] = [x]$$
$$[1][x] = [x]$$

が成立する。

また、加法についての逆元は $-[x] = [-x]$ で定まる。例えば $[2] + [1] = [3] = [0]$ なので、$-[2] = [1]$ である。

乗法の逆元については、この場合には $[2][2] = [4] = [1]$ となるから $[2]^{-1} = [2]$ である。

ここで記号 $[k]$ について注意しておく。上でも述べたように、$[1]=[4]=[-2]$ など同じものを表記する方法が複数ある。つまり、同じ数を表現する方法が一通りではない・しかしある一定の規則に基づいて異なる表記を「同じ数」であるとみなす。

同じ数について複数の表記が存在することは、例えば通常の有理数（分数）の計算で $\frac{1}{2}=\frac{2}{4}=\frac{3}{6}$ などとなるのと同様。この場合、「約分」して一致する表記は「同じ数」とみなすという規則を定めている。

例 2. $\mathbb{Z}/(5)$ を整数全体を 5 で割ったあまりが等しいものを同一視してできる集合とする。つまり、要素としては $\{[0],[1],[2],[3],[4]\}$ の 5 つからなる有限集合。

例えば $[2]+[4]=[6]=[1],[3][4]=[12]=[2]$ のように計算できる。これが結合法則、分配法則、交換法則を満たすことは整数の場合の計算からわかり、単位元を持つことも上と同様。

乗法の逆元についてだけ注意が必要なので説明しておく。$[2][3]=[6]=[1],[4][4]=[16]=[1]$ であるから、$[2]^{-1}=[3],[3]^{-1}=[2],[4]^{-1}=[4]$ である。

より一般に次が成り立つ。

命題 1. p を素数とする。剰余環 $\mathbb{Z}/p=\{[0],[1],\dots,[p-1]\}$ は体になる。特に $[k]\neq[0]$ なら $[k][x]=[1]$ となる整数 x が存在する。

証明. $[k]\neq[0]$ なので k と p は互いに素。したがってユークリッドの互除法から $kx+py=1$ となる整数 x,y が存在する。このとき、$[kx+py]=[k][x]+[p][y]=[k][x]=1$ となる。 □

素数でない整数についての余りを考えて同様な構成を行っても体にはならないことに注意しよう。

例 3. 上と同様に $\mathbb{Z}/(6)$ を定めると、ここでは $[2][3]=[6]=[0]$ となる。もし $[2]$ の乗法についての逆元 $[2]^{-1}$ が存在すると、$[2]^{-1}[2][3]=[2]^{-1}[0]=[0]$ となることから $[3]=[0]$ となってしまう。したがって、$[2]$ には乗法についての逆元が存在しないことがわかる。したがって、これは体ではない。

素数 p について上で述べた方法で定まる $\mathbb{Z}/(p)$ を $\mathbb{F}_p$ とかく。つまり $\mathbb{F}_p=\{[0],[1],\dots,[p-1]\}$ である。これ以外の有限体の作り方として以下では（一見異なるが本質的には差のない）二つの方法を紹介する。

まず、上が整数全体を素数で割ったあまりを考えたことの類似として、例えば $i^2=-1$ として $\mathbb{Z}[i]=\{a+bi\in\mathbb{C}\mid a,b\in\mathbb{Z}\}$ の剰余を考えてみよう。

例 4. $\mathbb{Z}[i]$ の要素を a,b を 3 で割ったあまりが共に等しい時に同一視したものを $\mathbb{Z}[i]/(3)$ とかく。集合としては $\{[0],[1],[2],[i],[1+i],[2+i],[2i],[1+2i],[2+2i]\}$ と 9 個の要素をもつ。

これが体になることを見てみよう。加法と乗法を

$$[a+bi]+[c+di]=[(a+b)+(c+d)i]$$
$$[a+bi][c+di]=[(ac-bd)+(ad+bc)i]$$

と定めると、これが結合法則、分配法則、交換法則を満たし、$[0],[1]$ がそれぞれ加法と乗法の単位元となる。

$[1+i]$ の積についての逆元を求めよう。$(1+i)(1-i)=2$ であり、$[2][2]=[1]$ であるから、$[1+i][1-i][2]=[1]$ となる。つまり、$[1+i]^{-1}=[2-2i]=[2+i]$ となる。これ以外の要素についても同様に逆元が計算できる。$[a+bi]$ に対し、a,b いずれも 3 の倍数でなければ a^2+b^2 を 3 で割ったあまりが 1 または 2 であるから、自分自身が $[a^2+b^2]$ の逆元、つまり $[a^2+b^2][a^2+b^2]=[1]$ となる。よって、$[a+bi][(a-bi)(a^2+b^2)]=[1]$ となる。

ただし、この構成法では実は注意が必要である。

例 5. 上と同じように $\mathbb{Z}[i]/(5)$ を考えてみると、これは体にならない。$[1+2i][1-2i]=[5]=[0]=0$ なので、0 でない要素の積が 0 となってしまい、これらに逆元が存在しない。

これは 5 が $\mathbb{Z}[i]$ においては「素数でない」ことの反映といえる。$\mathbb{Z}/(6)$ が体でないことを思い出そう。

例 6. そこで代わりに $\mathbb{Z}[\sqrt{2}]/(5)$ を考える。これは $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\in\mathbb{C}\mid a,b\in\mathbb{Z}\}$ の要素を a,b を 5 で割ったあまりが共に等しいときに同一視する。

これが体になることを確かめる。$[a+b\sqrt{2}][a-b\sqrt{2}]=[a^2+2b^2]$ であるが、平方数を 5 で割った余りが $1,4$ のいずれかであることから、a^2+2b^2 が 5 で割り切れるとしたら a も b も 5 で割り切れることがわかる。したがって $N=a^2+2b^2$ は 5 と互いに素な整数だから $Nx+5y=1$ となる整数 x,y が存在し、$[N][x]=[1]$ となる。

2 多項式環の剰余

もう一つの作り方として、$\mathbb{R}$ から $\mathbb{C}$ を作る時に方程式 $x^2+1=0$ の解 $i=\sqrt{-1}$ を付け加えたのと同じことをする。この方法では多項式の剰余を考えるという方法で実現する。実数係数の多項式の集まり $\mathbb{R}[x]$ について、(x^2+1) で割ったあまりが等しいものを同一視することで新しい集合 $\mathbb{R}[x]/(x^2+1)$ を作ろう。要素は $[ax+b]$ という形で表せる。このとき、演算は

$$[ax+b]+[cx+d]=[(a+c)x+(b+d)]$$
$$[ax+b][cx+d]=[acx^2+(ad+bc)x+bd]=[(ad+bc)x+bd-ac]$$

となる。ここでは x^2+ax+b を x^2+1 で割ったあまりが $ax+b-1$ であることを用いて計算した。

これは複素数の演算

$$(ai+b)+(ci+d)=(a+c)i+(b+d)$$
$$(ai+b)(ci+d)=(-ac+bd)+(ad+bc)i$$

と同じものになっている。

これと同様にして $\mathbb{F}_p$ で既約な多項式の根を付け加えることで新しい体を作る。多項式の集まりにおいてもユークリッドの互除法が使えることを思い出す。

例 7. $x^2+1=0$ は $\mathbb{F}_3$ において解を持たないので次数が 2 だから既約。剰余環 $\mathbb{F}_3[x]/(x^2+1)$ は体になる。

具体的に計算してみると、

$$[x+1][x+2]=[x^2+3x+2]=[x^2+2]=[-1+2]=[1]$$
$$[2x+1][2x+2]=[4x^2+6x+2]=[x^2+2]=[-1+2]=[1]$$

などとなる。$x=\sqrt{-1}$ と思って計算すればよい。

これを $\mathbb{F}_3[i]$ と書くことにしよう。

$\mathbb{F}_5$ においては $x^2+1=0$ が解 $x=[2],[3]$ を持つため、この式による剰余は体とならない。

例 8. x^2-2 は $\mathbb{F}_5$ において解を持たないので次数が 2 だから既約。剰余環 $\mathbb{F}_5[x]/(x^2-2)$ は体になる。

具体的に計算してみると、

$$[x+1][2x+3]=[2x^2+5x+3]=[2x^2+3]=[4+3]=[2]$$
$$[2x+1][3x+4]=[6x^2+11x+4]=[x^2+x+4]=[2+x+4]=[x+1]$$

などと計算できる。$x=\sqrt{2}$ と思って計算すればよい。

これを $\mathbb{F}_5[\sqrt{2}]$ と書くことにしよう。

例 9. $x^3+x^2+1=0$ は $\mathbb{F}_2$ において解を持たず次数が 3 なので既約。剰余環 $\mathbb{F}_2[x]/(x^3+x^2+1)$ は体となる。この解のうち一つを α とする。これを用いて上の体は集合として

$$\{[0],[1],[\alpha],[\alpha+1],[\alpha^2],[\alpha^2+\alpha],[\alpha^2+1],[\alpha^2+\alpha+1]\}$$

と表すことができる。

具体的に計算してみると、

$$[\alpha+1][\alpha+1]=[\alpha^2+2\alpha+1]=[\alpha^2+1]$$
$$[\alpha^2+1][\alpha+1]=[\alpha^3+\alpha^2+\alpha+1]=[\alpha][\alpha]^3=[\alpha^3] \qquad =[-\alpha^2-1]=[\alpha^2+1]$$

などと計算できる。

これを $\mathbb{F}_2[\alpha]$ と書くことにしよう。実は $x^3+x^2-2x-1=0$ の実数における解のうち一つは $2\cos\dfrac{2\pi}{7}$ である。

多項式環の剰余環については龍孫江さんの動画で丁寧に解説されているので、そちらを参考にしてください。

（特別編）多項式環の剰余環が体になる条件 https://www.youtube.com/watch?v=NztSl_vxeXI

3 有限体の要素の個数

上で見た例は全て要素の個数が素数のベキ乗である。実はこのことは一般に成り立つ。

命題 2. F が有限体とする。1 を足して 0 になる最小の回数 n（つまり加法群としての 1 の位数）は必ず素数である。

証明. $n=lm$ とすると、$lm=0$ となる。n の最小性から F においては $l\neq 0, m\neq 0$ であるが、体なので p,k は乗法逆元をもつ。これは矛盾。 □

定義 1. これを F の標数という。

つまり、有限体の標数は必ず素数 p になる。

命題 3. 有限体 F の標数が p のとき、F の要素の個数はある自然数 n について p^n となる。

証明. F が標数 p であれば $\mathbb{F}_p\subset F$ であるが、この時 F は $\mathbb{F}_p$ 上の線形空間になる。要素の個数が有限だから、これは有限次元である。この次元を n とすると、集合として F から $\mathbb{F}_p^n$ への全単射（線形写像としての同型）が存在するので、F の要素の個数は p^n である。 □

例 10. $\mathbb{F}_3[i]$ は $\mathbb{F}_3$ 上 2 次元のベクトル空間で基底としては例えば $1, i$ を取れる。要素は $3^2 = 9$ 個の有限体。

例 11. $\mathbb{F}_5[\sqrt{2}]$ は $\mathbb{F}_5$ 上 2 次元のベクトル空間で基底としては例えば $1, \sqrt{2}$ を取れる。要素は $5^2 = 25$ 個の有限体。

例 12. $\mathbb{F}_2[\alpha]$ は $\mathbb{F}_2$ 上 3 次元のベクトル空間で基底としては例えば $1, \alpha, \alpha^2$ を取れる。要素は $2^3 = 8$ 個の有限体。

これらについては、龍孫江さんが体の定義から丁寧に解説されているので、そちらも参考にしていただくとよいと思う。

（特別編）体論：有限体の要素の数 https://www.youtube.com/watch?v=f54XvG2LKdg&t=904s

（特別編）素数個の要素をもつ体の構成 https://www.youtube.com/watch?v=UPf0lf0GQ7U

4 有限体の乗法群

有限体 F は体なので 0 以外には積についての逆元が存在する。このことから、$F \setminus \{0\}$ は積に関して群となる。これを F の乗法群と呼び $F^\times$ と表す。

ここでの目標はこの乗法群 $F^\times$ の構造を調べることである。結論はこれが位数 $q-1$ の巡回群となること、つまりある $a \in \mathbb{F}_q^\times$ を用いて $\mathbb{F}_q^\times = \{1, a, a^2, \ldots, a^{q-2}\}$ と書けることを示す。

まずはこの事実について、いくつか具体例を見ておこう。

例 13. $\mathbb{F}_3^\times = \{[1], [2]\}$ について $[2]^2 = [4] = [1]$ である。

例 14. $\mathbb{F}_5^\times = \{[1], [2], [3], [4]\}$ について。$[2]^2 = [4], [2]^3 = [8] = [3]$ であり、

$$\mathbb{F}_5^\times = \{[1], [2], [2]^2 = [4], [2]^3 = [3]\}$$

と書ける。

例 15. $\mathbb{F}_7^\times = \{[1], [2], [3], [4], [5], [6]\}$ について。$[2]^2 = [4], [2]^3 = [8] = [1]$ なので、これを用いては全ての要素を作れない。一方で $[3]^2 = [9] = [2]$ であり、

$$\begin{aligned}
[3]^3 &= [2][3] = [6] \\
[3]^4 &= [2]^2 = [4] \\
[3]^5 &= [4][3] = [12] = [5] \\
[3]^6 &= [2]^3 = [1]
\end{aligned}$$

となる。よって

$$\mathbb{F}_7^\times = \{[1], [3], [3]^2 = [2], [3]^3 = [6], [3]^4 = [4], [3]^5 = [5]\}$$

とかける。

例 16. $(\mathbb{F}_3[\sqrt{-1}])^\times$ について考える。まず上で見たように $[2]^2 = [1]$ である。また、通常の複素数と同様に $[\sqrt{-1}]^2 = [-1] = [2], [\sqrt{-1}^4] = 1$ である。実は $\{[1], [\sqrt{-1}], [2], [2\sqrt{-1}]\}$ が $x^4 = x$ の解全体。この外にある $\mathbb{F}_3[\sqrt{-1}]$ の要素を適当に取ると、その位数は 8 となることが（計算せずとも群の一般論から）わかる。あるい

は $\frac{1+i}{\sqrt{2}}$ が $\mathbb{C}$ における 1 の 8 乗であることを思い出すと、$[\frac{1+\sqrt{-1}}{\sqrt{2}}] = [\frac{1+\sqrt{-1}}{\sqrt{-1}}] = [1+\sqrt{-1}][2\sqrt{-1}] = [1+2\sqrt{-1}]$ として、

$$
\begin{aligned}
[1+2\sqrt{-1}]^2 &= [1+4\sqrt{-1}-4] = [\sqrt{-1}] \\
[1+2\sqrt{-1}]^3 &= [\sqrt{-1}][1+2\sqrt{-1}] = [\sqrt{-1}+2] = [2+\sqrt{-1}] \\
[1+2\sqrt{-1}]^4 &= [\sqrt{-1}]^2 = [-1] = [2] \\
[1+2\sqrt{-1}]^5 &= [2][1+2\sqrt{-1}] = [2+4\sqrt{-1}] = [2+\sqrt{-1}] \\
[1+2\sqrt{-1}]^6 &= [\sqrt{-1}]^3 = [-\sqrt{-1}] = [2\sqrt{-1}] \\
[1+2\sqrt{-1}]^7 &= [2\sqrt{-1}][1+2\sqrt{-1}] = [2\sqrt{-1}-4] = [2+2\sqrt{-1}] \\
[1+2\sqrt{-1}]^8 &= [\sqrt{-1}]^4 = [1]
\end{aligned}
$$

となり、$\mathbb{F}_3[\sqrt{-1}]$ の要素が全て $[1+2\sqrt{-1}]^n$ の形で表すことができた。

例 17. $\mathbb{F}_5[\sqrt{2}]^\times$ を考える。この群の位数は 24 である。$\mathbb{F}_5^\times$ は $[2]$ が生成する。また、$[\sqrt{2}]^2 = [2]$ だから、これは位数 8 の要素。

一方で、$\frac{-1+\sqrt{-3}}{2}$ が $\mathbb{C}$ における 1 の 3 乗根であることから、$[\frac{-1+\sqrt{-3}}{2}] = [4+\sqrt{2}][3] = [2+3\sqrt{2}]$ を考えると、

$$
\begin{aligned}
[2+3\sqrt{2}]^2 &= [4+12\sqrt{2}+18] = [2+2\sqrt{2}] \\
[2+3\sqrt{2}]^3 &= [2+2\sqrt{2}][2+3\sqrt{2}] = [4+10\sqrt{2}+12] = [1]
\end{aligned}
$$

となるから、これは位数 3 の要素。

このことから $[\sqrt{2}][2+3\sqrt{2}] = [1+2\sqrt{2}]$ が位数 24 の要素であることがわかる。実際、$([\sqrt{2}][2+3\sqrt{2}])^n = [1]$ とすると、$[2+3\sqrt{2}]^n = [\sqrt{2}]^{-n}$ となる。上の具体的な計算から

$$
\begin{aligned}
\{[2+3\sqrt{2}]^n \in \mathbb{F}_5[\sqrt{2}] \mid n \in \mathbb{Z}\} &= \{[1], [2+3\sqrt{2}], [2+\sqrt{2}]\} \\
\{[\sqrt{2}]^n \in \mathbb{F}_5[\sqrt{2}] \mid n \in \mathbb{Z}\} &= \{[1], [\sqrt{2}], [2], [2\sqrt{2}], [4], [4\sqrt{2}], [3], [3\sqrt{2}]\}
\end{aligned}
$$

だから共通部分は $[1]$ のみで、$[\sqrt{2}]^{-n} = [1] = [2+3\sqrt{2}]^n$ となるから、n は 3 の倍数であり 8 の倍数でもある。よって n は 24 の倍数となり、$[1+2\sqrt{2}]$ は 24 乗して初めて 1 になりしかもすべて異なることもわかる。

例 18. $\mathbb{F}_2[\alpha]^\times$ を考える。ここで $[\alpha^3+\alpha^2+1] = [0]$ であった。$[2] = [0]$ に注意すると $[\alpha^3] = [\alpha^2+1]$ が成り立つ。

これの乗法群の構造だが、$[\alpha]^7 = 1$ となることを確かめよう。これは群論の一般論から計算せずとも従うが、実際に順番に冪を計算してみると、

$$
\begin{aligned}
[\alpha]^3 &= [\alpha^2+1] \\
[\alpha]^4 &= [\alpha^2+1][\alpha] = [\alpha^3+\alpha] = [\alpha^2+\alpha+1] \\
[\alpha]^5 &= [\alpha^2+\alpha+1][\alpha] = [\alpha^3+\alpha^2+\alpha] = [\alpha+1] \\
[\alpha]^6 &= [\alpha+1][\alpha] = [\alpha^2+\alpha] \\
[\alpha]^7 &= [\alpha^2+\alpha][\alpha] = [\alpha^3+\alpha^2] = [1]
\end{aligned}
$$

となり、$\mathbb{F}_2[\alpha]^\times$ の全ての要素が $[\alpha]^n$ の形で表される。

命題 4. 有限体 F の乗法群 $F^\times$ は巡回群である。

証明. 位数の最大値を N とし、位数が N となる要素を一つとって $x \in F^\times$ とする。このとき、$x^N = 1$ であり、$x^m = 1$ なら m は N の倍数である。

まず $F^\times$ の要素の位数は全て N の約数であることを示す。$y \in F^\times$ が位数 k を持ち、k が N の約数でないとしよう。特に y のべきにとり直して k と N が互いに素としてよい。このとき $y^m = 1$ なら m は k の倍数である。

xy の位数を M とすると、$(xy)^M = x^M y^M = 1$ であるから $x^M = y^{-M}$ である。$x^{MN} = (y^{-M})^N = 1$ より MN は k の倍数だが、N と k は互いに素なので M は k の倍数。また、$(y^{-M})^k = x^{Mk} = 1$ より Mk は N の倍数となり、N と k が互いに素なので M は N の倍数でもある。よって M は Nk の倍数であるが、N が最大であることからこのような y は存在しないことがわかり、$F^\times$ の要素の位数は全て N の約数となる。

よって $F^\times$ の要素は全て $x^N = 1$ の解となる。$x^N = 1$ の解の個数は N なので、$F^\times$ の要素の個数は N 以下となり、一方で群 $F^\times$ の位数は $q-1$ だから $N = q-1$ となる。 □

5 有限体の一意性

ここでは、位数が同じ有限体は全て本質的に同じものになることを示す。

例 19. 位数が 9 の体 F について考えてみよう。まず F の標数は 3 なので、$\mathbb{F}_3$ を含む。$\mathbb{F}_3$ の要素は $x^3 = x$ を満たすが、この方程式の解はたかだか 3 個なので解全体が $\mathbb{F}_3$ と一致する。

$F^\times$ は位数が 8 の巡回群なので、特に $\alpha^4 = 1, \alpha^2 \neq 1$ となる α を取れる。これを用いて x に α を代入する写像 $\mathbb{F}_3[x] \to F$ を $f(x) \mapsto f(\alpha)$ を定めると、この α は $\alpha^2 = -1$ を満たすので準同型定理より $\mathbb{F}_3[x]/(x^2+1) \to F$ が単射になる。要素の個数が両辺共に 9 なので、これは同型となる。これは、前に作った体 $\mathbb{F}_3[\sqrt{-1}]$ とも同型である。

命題 5. 素数べき $q = p^n$ に対し、要素の個数が q の体は全て同型になる。

証明. F_1 と F_2 が共に位数 p^n をもつとする。

$F_1^\times$ は位数 $p^n - 1$ の巡回群で、ある $a \in F_1$ が存在して a^n で全て表せる。したがって $\mathbb{F}_p[x] \to F_1$ を $f(x) = f(a)$ で定義すると、これは全射となる。

F_1 の $\mathbb{F}_p$ 上の次元が n であることから、上の写像の核はある既約 n 次式 $g(x)$ で生成される。これを用いて同型 $F_1 \cong \mathbb{F}_p[x]/(g(x))$ が定まる。また $g(a) = 0$ であり、a を根に持つ多項式は全て $g(x)$ の倍数である。特に $a^{p^n-1} = 1$ だから $x^{p^n-1} - 1$ は $g(x)$ で割り切れる。

$F_2^\times$ も位数 $p^n - 1$ の巡回群であり、$x^{p^n-1} = 1$ の解全体と一致する。したがって特に $g(b) = 0$ となる $b \in F_2$ が存在する。この b を用いて $\mathbb{F}_p[x] \to F_2$ を $f(x) \mapsto f(b)$ と定めると、これは準同型定理と $g(x)$ の既約性から単射 $\mathbb{F}_p[x]/(g(x)) \to F_2$ を導き、位数を比べてこれが同型となる。

よって、F_1, F_2 がいずれも $\mathbb{F}_p[x]/g(x)$ と同型な体となることが証明できた。 □

要素の個数で体が（同型を除いて）決まってしまうことは龍孫江さんの動画
（特別編）有限体の一意性（13 分ごろから）https://www.youtube.com/watch?v=ei_89CwO99E
も参考にされるとよいと思います。

6　有限体のガロア理論

ガロア理論については改めて詳しく解説する予定ですが、ここでは最低限の事実だけ並べておきます。

二項係数 ${}_pC_k$ が $0 < k < p$ において p で割り切れることから、標数 $p > 0$ の体において $(x+y)^p = x^p + y^p$ が成立する。$\mathbb{F}_p$ の要素については $x^p = x$ であるから、$f(x) \in \mathbb{F}_p[x]$ に対しては $f(x)^p = f(x^p)$ となる。

$a \in \mathbb{F}_{p^n}$ を乗法群 $\mathbb{F}_{p^n}^\times$ の生成元とする。すると $a^{p^n} = a$ である。a の $\mathbb{F}_p$ 係数の最小多項式を $f(x)$ とすると $f(a) = 0$ であり、上に述べたことから $f(a)^p = f(a^p) = 0$ となる。よって $a^p, a^{p^2}, \ldots, a^{p^{n-1}}$ が $f(x) = 0$ の他の解を与え、これが共役。

この p 乗写像 $\phi(x) = x^p$ が根の入れ替えを定め、これがガロア群を生成する。$\mathbb{F}_{p^n}/\mathbb{F}_p$ は常にガロア拡大で、ガロア群は $x \mapsto x^p$ が生成する位数 n の巡回群となる。$\phi(x)$ をフロベニウス写像と呼ぶ。

命題 6. 有限体 $\mathbb{F}_p$ に対し、次数 n ごとに同型をのぞいてただ一つのガロア拡大 $\mathbb{F}_{p^n}/\mathbb{F}_p$ が存在し、有限次拡大はこれで全て。$\mathbb{F}_{p^n}/\mathbb{F}_p$ のガロア群は巡回群であり、生成元としてフロベニウス写像 $\phi(x) = x^p$ が取れる。

さて、有限体 $\mathbb{F}_p$ に対して、1 の p と素な冪根を全て集めた体を $\bigcup_{p\nmid n} \mathbb{F}_p[\mu_n] = \mathbb{F}_{p^\infty}$ と書くことにする。これが $\mathbb{F}_p$ の代数閉包を与える。

$\mathbb{F}_{p^\infty}$ の自己同型としてフロベニウス写像 $\phi : x \mapsto x^p$ の整数乗 $\phi^n(x) = x^{p^n}$ があるが、これのある種の極限も自己同型を定めることが以下のようにわかる。

$\mathbb{F}_{p^\infty} = \bigcup_n \mathbb{F}_{p^n}$ であるから、$\mathbb{F}_{p^n}$ の自己同型をうまく整合的になるように並べることで $\mathbb{F}_{p^\infty}$ の自己同型を作ることができる。つまり各自然数 n に対して、$\phi^{a_n} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ を用意して、その列 $\{a_n\}$ を考える。各々 a_n は $\mathbb{F}_{p^n}$ において $\phi^n = 1$ であることから　$\bmod n$ のみに依存する。整合性というのは、n が m の倍数であるとき、$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ である関係をうまく保つことを要請するもの。つまり、$x \in \mathbb{F}_{p^m}$ に対して $\phi^{a_n}(x) = \phi^{a_m}(x)$ が成立する必要がある。これは $a_n \mod m = a_m$ という条件に他ならない。

つまり、$\mathbb{F}_{p^\infty}$ の自己同型を定めるには、$a_n \in \mathbb{Z}/n$ の列 $\{a_n\}$ であって、$m \mid n$ に対し $a_n \mod m = a_m$ となるものを与えればよい。

このような理由から有限体の絶対ガロア群、すなわち $\mathbb{F}_{p^\infty}$ の自己同型群が $\hat{\mathbb{Z}}$ と書かれる $\mathbb{Z}$ を「完備化」した群になることがわかる。

フロベニウス写像については以下の龍孫江さんの動画が参考になります。

体論：有限体の有限拡大 https://www.youtube.com/watch?v=CvxTUk82YHw

体論：正標数の体上のある多項式のガロア群（お詫び・訂正版）https://www.youtube.com/watch?v=gC1Jp1KXUrA

またガロア理論についてはこちらのテキストを参照してください。http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/infinite-Galois.pdf