More about finite fields: characteristic (§15.2), Frobenius map (§17.5)

Note $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$ with $\alpha := \bar{x}$

$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

has a copy of the subfield $\mathbb{F}_2 = \{0,1\}$ inside it, and it is a 3-dimensional $\mathbb{F}_2$-vector space like $(\mathbb{F}_2)^3$, which is why it has size $q = 2^3 = 8$.

PROPOSITION: Let $\mathbb{F}_q$ be any finite field with q elements. Then

(i) $q = p^d$ for some prime p, called the characteristic of $\mathbb{F}_q$

(ii) p is the smallest positive integer with $\underbrace{1+1+\cdots+1}_{p \text{ times}} = 0$ in $\mathbb{F}_q$

(iii) $\mathbb{F}_q$ contains $\mathbb{F}_p = \mathbb{Z}/p$ as a subfield, and this makes $\mathbb{F}_q$ into an $\mathbb{F}_p$-vector space of dimension d.

proof: Let m be the smallest positive integer for which $\underbrace{1+1+\dots+1}_{m \text{ times}} = 0$

(m exists since $1, 1+1, 1+1+1, \dots$ must eventually repeat in $\mathbb{F}_q$, and if $\underbrace{1+1+\dots+1}_{a \text{ times}} = \underbrace{1+1+\dots+1}_{b \text{ times}}$

then subtracting gives $\underbrace{1+1+\dots+1}_{m=b-a} = 0$).

We claim m is a prime p, otherwise if $m=ab$,

$$\underbrace{1+1+\dots+1}_{m=ab \text{ times}} = \underbrace{(1+1+\dots+1)}_{a \text{ times}}\underbrace{(1+1+\dots+1)}_{b \text{ times}}$$

$\Rightarrow$ either $\underbrace{1+1+\dots+1}_{a} = 0$ or $\underbrace{1+1+\dots+1}_{b} = 0$,

since $\mathbb{F}_q$ is a field

contradicting m being smallest.

Then it's not hard to see that inside $\mathbb{F}_q$ one has $\mathbb{F}_p = \{0, 1, 1+1, 1+1+1, \dots, \underbrace{1+1+\dots+1}_{p-1 \text{ times}}\} = \mathbb{Z}/p$ as a subring and a subfield.

One sees that this makes $\mathbb{F}_q$ an $\mathbb{F}_p$-vector space.

Then if one picks some $\mathbb{F}_p$-basis $v_1, v_2, \ldots, v_d$ for $\mathbb{F}_q$ where $d = \dim_{\mathbb{F}_p}(\mathbb{F}_q)$, we know the map

$$\begin{aligned}(\mathbb{F}_p)^d &\longrightarrow \mathbb{F}_q \\ \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_d \end{bmatrix} &\longmapsto c_1 v_1 + c_2 v_2 + \cdots + c_d v_d\end{aligned}$$

is a bijection, so $q = \#\mathbb{F}_q = \#(\mathbb{F}_p)^d = p^d$ $\blacksquare$

A lot of further theory of finite fields (and coding theory, e.g. BCH codes) uses a charming feature of $\mathbb{F}_q$:

PROPOSITION: ("The Freshman Dream") In $\mathbb{F}_q$ and in $\mathbb{F}_q[x]$ with $q = p^d$ for p prime, one has $(\alpha + \beta)^p = \alpha^p + \beta^p$

EXAMPLES:

(1) In $\mathbb{F}_5$, $(1+2)^5 = 3^5 = 243 = 3$

$1^5 + 2^5 = 1 + 32 = 33 = 3$

(2) In $\mathbb{F}_3[x]$, $(x^4+1)^3 = x^{12} + \cancel{3}x^8 + \cancel{3}x^4 + 1$

$= x^{12} + 1$

proof of Freshman Dream:

Note that

$$(\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta^1 + \binom{p}{2}\alpha^{p-2}\beta^2 + \dots + \binom{p}{p-1}\alpha^1\beta^{p-1} + \beta^p$$

CLAIM: These coefficients all vanish in $\mathbb{F}_q$,

that is $\binom{p}{k} = 0$ for $1 \le k \le p-1$,

gives a factor of p

$$\text{because } \binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)(p-2)\cdots\cdots(p-k+1)}{k(k-1)(k-2)\cdots\cdots(1)}$$

none of these has a factor of p that could cancel that factor of p in the numerator.

So $(\alpha+\beta)^p = \alpha^p + \beta^p$ $\blacksquare$

This leads to an interesting map on $\mathbb{F}_q$ called the Frobenius map

$$\begin{aligned} \mathbb{F}_q &\xrightarrow{\Phi} \mathbb{F}_q \\ \alpha &\longmapsto \Phi(\alpha) := \alpha^p \end{aligned}$$

where $q = p^d$

ACTIVE LEARNING:

(1) Let $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$ with $\alpha := \bar{x}$

$$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

Compute $\Phi(\beta) = \beta^2$ for every $\beta \in \mathbb{F}_8$

---

(2) Draw arrows

$$\beta \overset{\Phi}{\longmapsto} \underset{\Phi(\beta)}{\overset{\beta^2}{\shortparallel}} \overset{\Phi}{\longmapsto} \underset{\Phi^2(\beta) = \Phi(\Phi(\beta))}{\overset{\beta^4}{\shortparallel}} \longmapsto \cdots$$

showing how Φ maps the 8 elements of $\mathbb{F}_8$ and breaks it into orbits.

Compute the polynomials

$$(x-\beta)(x-\Phi(\beta))(x-\Phi^2(\beta))\cdots \quad \text{in } \mathbb{F}_8[x]$$

for each orbit.

---

(3) Factor $y^8 - y$ into irreducibles in $\mathbb{F}_2[y]$, and in $\mathbb{F}_8[y]$.

PROPOSITION:

The Frobenius map $\mathbb{F}_q \xrightarrow{\Phi} \mathbb{F}_q$ for $q=p^d$
$\alpha \longmapsto \alpha^p$

(i) is a bijection,

(ii) respecting + and ×, that is,

$$\Phi(\alpha+\beta)=\Phi(\alpha)+\Phi(\beta)$$
$$\Phi(\alpha\beta)=\Phi(\alpha)\Phi(\beta)$$

(iii) fixes every $\alpha\in\mathbb{F}_p$ $(\subset \mathbb{F}_q)$

i.e. $\Phi(\alpha)=\alpha \;\; \forall \alpha\in\mathbb{F}_p$

(iv) has $\Phi^d(\alpha)=\alpha \;\; \forall \alpha\in\mathbb{F}_q$

---

proof: Let's check (iv) first. To compute $\Phi^d(\alpha)$,

note
$$\Phi(\alpha)=\alpha^p$$
$$\Phi^2(\alpha)=\Phi(\Phi(\alpha))=\Phi(\alpha^p)=(\alpha^p)^p=\alpha^{p^2}$$
$$\Phi^3(\alpha)=\Phi(\alpha^{p^2})=(\alpha^{p^2})^p=\alpha^{p^3}$$
$$\Phi^k(\alpha)=\alpha^{p^k}$$

so
$$\Phi^d(\alpha)=\alpha^{p^d}=\alpha^q=\alpha\cdot\alpha^{q-1}=\begin{cases}0 & \text{if } \alpha=0\\ \alpha\cdot 1=\alpha & \text{if } \alpha\in\mathbb{F}_q^\times\end{cases}$$
$$=\alpha \;\; \forall \alpha\in\mathbb{F}_q.$$

Once we know $\Phi^d(\alpha)=\alpha$ as in (iv), then Φ is a bijection as in (i), since Φ^{d-1} is its inverse bijection:

$$(\Phi \circ \Phi^{d-1})(\alpha) = \Phi^d(\alpha) = \alpha$$
$$(\Phi^{d-1} \circ \Phi)(\alpha) = \Phi^d(\alpha) = \alpha$$

Also, (iii) is just the $d=1$ special case of (iv).

And (i) is checked via the Freshman Dream for $+$ $\left[\Phi(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = \Phi(\alpha)+\Phi(\beta)\right]$

and $\times$ is easy:

$$\Phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p \beta^p = \Phi(\alpha)\Phi(\beta) \quad \boxtimes$$

EXAMPLES

(1) In $\mathbb{F}_3[x]$, x^2+x+2 is irreducible (Why?), so

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+x+2) \text{ is a field, with } \beta = \bar{x}$$
$$= \{0, 1, 2, \beta, \beta+1, \beta+2, 2\beta, 2\beta+1, 2\beta+2\}$$

and Frobenius map

$$\begin{array}{ccc} \mathbb{F}_9 & \xrightarrow{\Phi} & \mathbb{F}_9 \\ \alpha & \longmapsto & \alpha^3 \end{array}$$

having orbits

$$0 \circlearrowleft \qquad \beta \rightleftarrows \beta^3 = \beta(\beta^2) = \beta(2\beta+1) = 2\beta^2+\beta$$
$$= 2(2\beta+1)+\beta$$
$$= 2\beta+2$$

$$1 \circlearrowleft \qquad \beta+1 \rightleftarrows \beta^3+1 = 2\beta+2+1$$
$$= 2\beta$$

$$-1 = 2 \circlearrowleft \qquad \beta+2 \rightleftarrows \beta^3+2^3 = \beta^3+2 = 2\beta+2+2 = 2\beta+1$$

$$(y-\beta)(y-\beta^3) = (y-\beta)(y-(2\beta+2)) = y^2-2y+\beta(2\beta+2)$$
$$= y^2+y+2$$

$$(y-(\beta+1))(y-2\beta) = y^2-y+2 = y^2+2y+2$$

quadratic irreducibles in $\mathbb{F}_3[x]$

$$(y-(\beta+2))(y-(2\beta+1)) = y^2+1$$

and one can check

$$y^9-y = y(y^8-1) = y(y^2-1)(y^6+y^4+y^2+1)$$
$$= \underbrace{y(y-1)(y+1)}_{\text{linear irreducibles in } \mathbb{F}_3[y]}\underbrace{(y^2+y+2)(y^2+2y+2)(y^2+1)}_{\text{quadratic irreducibles in } \mathbb{F}_3[y]}$$

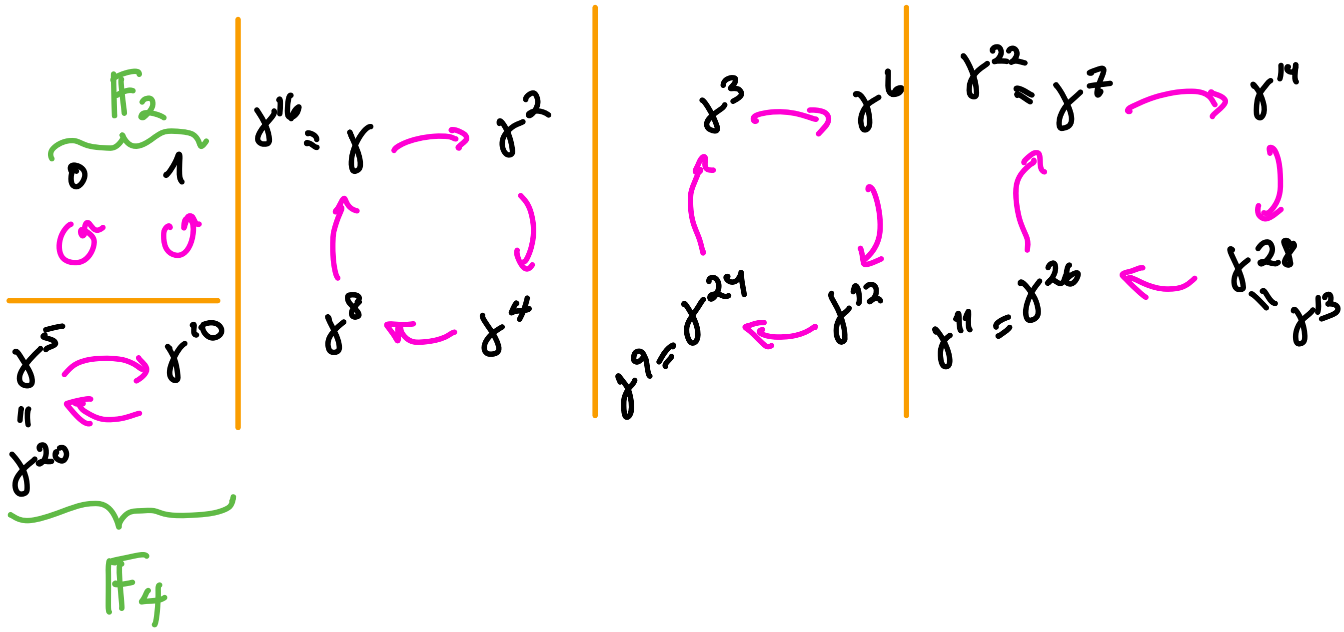
$$= y\cdot(y-1)\cdot(y-2)\cdot(y-\beta)(y-\Phi(\beta))\cdot(y-(\beta+1))(y-\Phi(\beta+1))\cdot(y-(\beta+2))(y-\Phi(\beta+2))$$

Φ Φ Φ Φ Φ Φ

(2) $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4+x+1)$ with $\gamma = \overline{x}$ a primitive root,

$$= \{0, \underset{\underset{\gamma^{15}}{\|}}{1}, \gamma, \gamma^2, \gamma^3, \dots, \gamma^{13}, \gamma^{14}\}$$

It has Frobenius map $\begin{array}{ccc} \mathbb{F}_{16} & \xrightarrow{\Phi} & \mathbb{F}_{16} \\ \alpha & \longmapsto & \alpha^2 \end{array}$ with orbits



and one can check

$$y^{16} - y = y(y+1)(y^2+y+1)(y^4+y+1)(y^4+y^3+y^2+y+1)(y^4+y^3+1) \text{ in } \mathbb{F}_2[x]$$

$$= y(y+1)\,(y-\gamma^5)(y-\gamma^{10})\,(y-\gamma)\cdot(y-\gamma^2)\cdot(y-\gamma^4)\cdot(y-\gamma^8)\cdot(y-\gamma^3)(y-\gamma^6)(y-\gamma^{12})(y-\gamma^9)\cdot(y-\gamma^7)(y-\gamma^{14})(y-\gamma^{13})(y-\gamma^{11})$$

Some general facts about a finite field $\mathbb{F}_q$ that we won't prove, but are not that hard:

THEOREM:

- One can build a finite field $\mathbb{F}_q$ of size $q=p^d$ for every prime p and power d, that is, there exist irreducible polynomials $f(x) \in \mathbb{F}_p[x]$ of every degree d, to build $\mathbb{F}_q = \mathbb{F}_p[x]/(f(x))$

- They are all isomorphic as fields, that is, $\exists$ a bijection $\mathbb{F}_q \xrightarrow{f} \mathbb{F}_q'$ with $f(\alpha+\beta) = f(\alpha)+f(\beta)$, $f(\alpha\beta) = f(\alpha)f(\beta)$ whenever fields $\mathbb{F}_q, \mathbb{F}_q'$ have same size q.

- In $\mathbb{F}_q[x]$, $x^q - x = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_q)$ if $\mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$

  In $\mathbb{F}_p[x]$, $x^q - x = g_1(x) \cdots g_m(x)$ where $g_i(x)$ are all the irreducibles in $\mathbb{F}_p[x]$ whose degree divides d (with $q=p^d$)

- The Φ-orbits on $\mathbb{F}_q$ are the sets of roots of the $g_i(x)$

- $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^{d'}} \iff d \mid d'$