Finite fields (Chap. 11)

Some of our new rings $\mathbb{F}_p[x]/(f(x))$ actually turn out to be new (finite) fields $\mathbb{F}_q$, with $q = p^{\deg(f)}$.

EXAMPLES Let's write the multiplication tables for

$R_1 = \mathbb{F}_2[x]/(x^2+x+1)$ versus $R_2 = \mathbb{F}_2[x]/(x^2+x)$

x^2+x+1: irreducible in $\mathbb{F}_2[x]$ (Why?)

x^2+x: reducible in $\mathbb{F}_2[x]$ (Why?)

renaming $\alpha := \bar{x}$, so

$R_1 = \mathrm{span}_{\mathbb{F}_2}\{1,\alpha\}$

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

with $\alpha^2+\alpha+1=0$

i.e. $\alpha^2 = \alpha+1$

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

A field!

renaming $\beta := \bar{x}$, so

$R_2 = \mathrm{span}_{\mathbb{F}_2}\{1,\beta\}$

$\{0, 1, \beta, \beta+1\}$

with $\beta^2+\beta=0$

i.e. $\beta^2 = \beta$

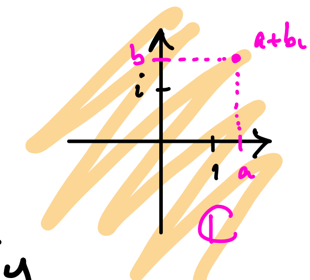
$\times$	0	1	β	$\beta+1$
0	0	0	0	0
1	0	1	β	$\beta+1$
β	0	β	β	0
$\beta+1$	0	$\beta+1$	0	$\beta+1$

Not a field!

Irreducibility for $f(x)$ is the key:

PROPOSITION: If $f(x)$ is irreducible in $\mathbb{F}[x]$ for $\mathbb{F}$ a field, then $\mathbb{F}[x]/(f(x))$ is also a field.

In particular, if $\mathbb{F} = \mathbb{F}_p$ has p elements then $\mathbb{F}[x]/(f(x))$ is a new field with p^d elements, where $d := \deg(f(x))$.



EXAMPLES

(1) x^2+1 in $\mathbb{R}[x]$ is irreducible,

so $\mathbb{R}[x]/(x^2+1)$ is a field, namely

$= \text{span}_{\mathbb{R}}\{1, \bar{x}\}$ our disguised version

of the field $\mathbb{C} = \text{span}_{\mathbb{R}}\{1, i\}$ with $i^2+1=0$

---

(2) x^2+x+1 in $\mathbb{F}_2[x]$ is irreducible, of degree 2,

so $\mathbb{F}_4 := \mathbb{F}_2[x]/(x^2+x+1) = \{0, 1, \alpha, \alpha+1\}$

with $\alpha := \bar{x}$ satisfying $\alpha^2+\alpha+1=0$

is a field with $p^d = 2^2 = 4$ elements

WARNING!: $\mathbb{F}_4 \neq \mathbb{Z}/4$

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, $\mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

(3) x^4+x+1 in $\mathbb{F}_2[x]$ is also irreducible (seen on HW) and has degree 4,

so $\mathbb{F}_{16} := \mathbb{F}_2[x]/(x^4+x+1)$ is a field with $2^4=16$ elements

$= \text{span}_{\mathbb{F}_2}\{1, \gamma, \gamma^2, \gamma^3\}$ where $\gamma := \bar{x}$ has $\gamma^4+\gamma+1=0$ i.e. $\gamma^4=\gamma+1$

$= \{0, 1, \gamma, \gamma+1, \gamma^2+1, \gamma^2+\gamma, \gamma^2+\gamma+1,$
$\gamma^3, \gamma^3+1, \gamma^3+\gamma, \gamma^3+\gamma+1, \gamma^3+\gamma^2+1, \gamma^3+\gamma^2+\gamma, \gamma^3+\gamma^2+\gamma+1\}$

---

proof of PROPOSITION:

To see $\mathbb{F}[x]/(f(x))$ is a field for $f(x)$ irreducible, consider any $\overline{g(x)} \neq \bar{0}$ in $\mathbb{F}[x]/(f(x))$, and find $\overline{g(x)}^{-1}$ as follows. Represent $\overline{g(x)}$ by some polynomial $g(x)$ with $\deg(g) < d = \deg(f)$, and then $GCD(g(x), f(x)) = 1$ since $g(x) \neq 0$ and f is irreducible.

Hence $1 = a(x)f(x) + b(x)g(x)$ in $\mathbb{F}[x]$

and $\bar{1} = \overline{b(x)}\,\overline{g(x)}$ in $\mathbb{F}[x]/(f(x))$,

that is $\overline{b(x)} = \overline{g(x)}^{-1}$.

When $\mathbb{F} = \mathbb{F}_p$, then we know we have a bijection

$$(\mathbb{F}_p)^d \longrightarrow \mathbb{F}_p[x]/(f(x))$$

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{bmatrix} \longmapsto c_0 + c_1\bar{x} + c_2\bar{x}^2 + \dots + c_{d-1}\bar{x}^{d-1}$$

so $\# \mathbb{F}_p[x]/(f(x)) = \#(\mathbb{F}_p)^d = p^d$ ▨

EXAMPLE Inside $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4+x+1)$

with $\gamma := \bar{x}$, who is $(\gamma^2)^{-1}$?

$\gamma^2 = \bar{x}^2$, so compute via (extended) Euclid

$$GCD(x^2, x^4+x+1) = GCD(x+1, x^2) = 1$$

$$\begin{array}{r} x^2 \\ x^2 \overline{) x^4+x+1} \\ \underline{x^4} \\ x+1 \end{array}$$

$x+1 = x^4+x+1 - x^2 \cdot x^2$

$1 = x^2 - (x+1)(x+1)$

$1 = x^2 - (x+1)(x^4+x+1 - x^2 \cdot x^2)$

$1 = (1-(x+1)\cdot x^2)x^2 - (x+1)(x^4+x+1)$

$= \underbrace{(x^3+x^2+1)}_{b(x)} \cdot x^2 - \underbrace{(x+1)}_{a(x)}(x^4+x+1)$

$$\begin{array}{r} x+1 \\ x+1 \overline{) x^2} \\ \underline{x^2+x} \\ x \\ \underline{x+1} \\ 1 \end{array}$$

$\Rightarrow (\gamma^2)^{-1} = \gamma^3 + \gamma^2 + 1$

Check: $\gamma^2(\gamma^3+\gamma^2+1) = \gamma^5 + \gamma^4 + \gamma^2$

$= \gamma \cdot (\gamma+1) + \gamma + 1 + \gamma^2 = \gamma^2 + \gamma + \gamma + 1 + \gamma^2 = 1$

REMARK Although not obvious, any two finite fields $\mathbb{F}_q$ and $\mathbb{F}_q'$ having the same size q will be isomorphic, meaning there is a bijection

$$\mathbb{F}_q \xrightarrow{f} \mathbb{F}_q'$$

with
$$f(\alpha+\beta) = f(\alpha) + f(\beta)$$
$$f(\alpha\beta) = f(\alpha) \cdot f(\beta).$$

EXAMPLE The two finite fields of size $q = 2^3 = 8$

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$ with $\alpha := \bar{x}$ | $\mathbb{F}_8' = \mathbb{F}_2[x]/(x^3+x^2+1)$ with $\beta := \bar{x}$

have an isomorphism, e.g., sending $\alpha \mapsto \beta^3$.

Check β^3 is a root of x^3+x+1 in $\mathbb{F}'$:

$$(\beta^3)^3 + \beta^3 + 1 = (x^2+1)^3 + (x^2+1) + 1$$
$$= x^6 + x^4 + \cancel{x^2} + 1 + \cancel{x^2} + \cancel{1} + \cancel{1}$$
$$= (x^3)^2 + x \cdot x^3 + 1$$
$$= (x^2+1)^2 + x(x^2+1) + 1$$
$$= x^4 + \cancel{1} + x^3 + x + \cancel{1}$$
$$= x^4 + x^3 + x = x(x^3+x^2+1) = x \cdot 0 = 0$$

Primitive roots & primitive polynomials (Chap. 15)

Recall that we showed long ago that if a ring R had units $R^\times := \{u \in R : u \text{ has a mult. inverse in } R\}$ finite of size N, then every $u \in R^\times$ had $u^N = 1$.

COROLLARY

In a finite field $\mathbb{F}_q$ with q elements, every $\alpha \neq 0$ has $\alpha^{q-1} = 1$

proof: $\mathbb{F}_q$ is a finite ring and $\#\mathbb{F}_q^\times = \#(\mathbb{F}_q - \{0\}) = q-1$. ∎

DEF'N: Call the smallest power $N = 1, 2, 3, \ldots$ for which $\alpha^N = 1$ the order of α in $\mathbb{F}_q$.

Call α a primitive element (root) in $\mathbb{F}_q$ if it has the largest possible order, namely $q-1$.

REMARK: We'll need primitive roots in $\mathbb{F}_q$ later to build Reed-Solomon codes with parameters $[q-1, t, q-t]$ for $t \leq q-1$.

 (with $n = q-1$, $k = t$, $d = q-t$)

EXAMPLES

(1) $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ has power table

α \ power	1	2	3	4	5	6	order of α
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

3, 5 are primitive

(2) In $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, $\alpha := \bar{x}$ is primitive

since $\alpha^2 = \alpha+1 \neq 1$,

but $\alpha^3 = 1$, so α has order $3 = q-1$

Also $\alpha+1$ is primitive, since $(\alpha+1)^2 = \alpha \neq 1$.

(3) In $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4+x+1)$,

$\gamma = \bar{x}$ is primitive, that is, of order $15 = q-1$

but $\gamma^3 = \bar{x}^3$ is not primitive,

since $(\gamma^3)^5 = \gamma^{15} = 1$

so γ^3 has order ≤ 5, not $q-1 = 16-1 = 15$.

Q: Do there exist primitive roots in every finite field $\mathbb{F}_q$? (Yes.)

Q: How to find them?

To answer these, start with some simple properties of order:

PROPOSITION:

(i) If $\alpha \in \mathbb{F}^\times$ has order d, then $\alpha^N = 1 \Leftrightarrow d \mid N$

(ii) Any power α^k of α has order dividing d (= order of α)

(iii) If $\alpha \in \mathbb{F}^\times$ has order $d = ef$, then α^f has order e.

(iv) If $\alpha_1, \alpha_2 \in \mathbb{F}^\times$ have orders d_1, d_2 with $GCD(d_1, d_2) = 1$ then $\alpha_1\alpha_2$ has order $d_1 d_2$.

proof:

(i): Certainly if $d \mid N$, say $N = de$, then $\alpha^N = \alpha^{de} = (\alpha^d)^e = 1^e = 1$

On the other hand, if $d \nmid N$ then $N = de + r$ with $1 \leq r \leq d-1$

so $\alpha^N = \alpha^{de+r} = (\alpha^d)^e \cdot \alpha^r = 1^e \cdot \alpha^r = \alpha^r \neq 1$ since $1 \leq r \leq d-1$.

(ii): If $\alpha^d = 1$, then $(\alpha^k)^d = \alpha^{kd} = (\alpha^d)^k = 1^k = 1$.

(iii): One has $(\alpha^f)^e = \alpha^{ef} = \alpha^d = 1$, and for $e' < e$ one has $(\alpha^f)^{e'} = \alpha^{e'f} \neq 1$ since $e'f < ef = d$.

(iv): $(\alpha_1\alpha_2)^N = 1 \iff \alpha_1^N \cdot \alpha_2^N = 1$

$\iff \underbrace{\alpha_1^N}_{\text{has order dividing } d_1} = \underbrace{\alpha_2^{-N}}_{\text{has order dividing } d_2}$

hence it has order dividing $1 = GCD(d_1, d_2)$
$\Rightarrow$ it is 1.

$\iff \alpha_1^N = 1 = \alpha_2^{-N}$

$\iff$ N is a multiple of d_1 and of d_2

$\iff d_1 d_2 \mid N$ ☒

THEOREM Every finite field $\mathbb{F}_q$ has a primitive root.

proof: Let $\ell := LCM\{\text{orders of all } \alpha \in \mathbb{F}_q^\times\}$

(e.g. for $\mathbb{F}_7 = \{\cancel{0}, 1, 2, 3, 4, 5, 6\}$
orders: 1 3 6 3 6 2
so $\ell = LCM(1,3,6,3,6,2) = 6$)

We claim that $\ell = q-1 \,(= \#\mathbb{F}_q^\times)$:

First note $\ell \mid q-1$ since every $\alpha \in \mathbb{F}_q^\times$ has $\alpha^{q-1} = 1$ and so its order divides $q-1$, and thus so does their LCM.

Second note $\ell \geq q-1$ because every $\alpha \in \mathbb{F}_q^\times$ has $\alpha^\ell = 1$ making it a root of $f(x) = x^\ell - 1$, which cannot have more than ℓ distinct roots.

This proves the claim that $\ell = q-1$.

Now we show $\exists$ some $\alpha \in \mathbb{F}_q^\times$ of order $\ell \,(= q-1)$, which would then be a primitive element.

Factor $\ell = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ into prime powers $p_i^{e_i}$ (for distinct primes).

Since $\ell = \mathrm{LCM}\{\text{orders of } \alpha \in \mathbb{F}_q^\times\}$, for each $i = 1, 2, \ldots, r$, there must be some $\alpha_i \in \mathbb{F}_q^\times$ with order divisible by $p_i^{e_i}$.

Then some power $\alpha_i^{d_i}$ has order exactly $p_i^{e_i}$.

And then $\alpha := \alpha_1^{d_1} \alpha_2^{d_2} \cdots \alpha_r^{d_r}$ will have order exactly $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = \ell$

using $\mathrm{GCD}(p_i^{e_i}, p_j^{e_j}) = 1$ repeatedly. $\boxtimes$

So primitive roots exist in $\mathbb{F}_q$,
but how to actually find one?
It's slightly tricky –
many elements of $\mathbb{F}_q^\times$ are primitive
(in fact, exactly $\varphi(q-1)$ of them; see §15.8).
So a strategy is to look for them via random search, once we have a quick test for primitivity:

PROPOSITION: (§16.3) $\alpha \in \mathbb{F}_q^\times$ is primitive

$$\iff \alpha^{\frac{q-1}{p}} \neq 1 \quad \forall \text{ primes } p \mid q-1$$

(i.e. if $q-1 = p_1^{e_1} \cdots p_r^{e_r}$ then check $\alpha^{\frac{q-1}{p_i}} \neq 1$ for $i = 1, 2, \ldots, r$)

proof: $\alpha \in \mathbb{F}_q^\times$ has $\alpha^{q-1} = 1$, so its order $d \mid q-1$,

and α is primitive $\iff$ d is not a proper divisor of $q-1$

$$\iff d \nmid \frac{q-1}{p} \quad \forall \text{ primes } p \mid q-1$$

$$\iff \alpha^{\frac{q-1}{p}} \neq 1 \quad \forall \text{ primes } p \mid q-1.$$

∎

EXAMPLES

(1) To check which elements in $\mathbb{F}_8^\times$ are primitive, factor $q-1 = 8-1 = 7$ into primes (only one!) and then $\alpha \in \mathbb{F}_8^\times$ is primitive

$$\Leftrightarrow \alpha^{\frac{q-1}{p}} = \alpha^{\frac{8-1}{7}} = \alpha \neq 1$$

i.e. the other 6 elements in $\mathbb{F}_8^\times - \{1\}$ are all primitive.

---

(2) In $\mathbb{F}_{16}^\times$, factor $q-1 = 16-1 = 15 = 3^1 \cdot 5^1$

and then $\alpha \in \mathbb{F}_{16}^\times$ is primitive

$$\Leftrightarrow 1 \neq \alpha^{\frac{16-1}{3}} = \alpha^5 \text{ and } 1 \neq \alpha^{\frac{16-1}{5}} = \alpha^3$$

So when we built $\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4+x+1)$, this is how we could check $\gamma := \bar{x}$ was primitive:

$\gamma^3 \neq 1$ (since $\mathbb{F}_{16}$ has $\mathbb{F}_2$-basis $\{1, \gamma, \gamma^2, \gamma^3\}$)

$\gamma^5 = \gamma \cdot \gamma^4 = \gamma(\gamma+1) = \gamma^2 + \gamma \neq 1$

REMARK: Once we know γ is primitive, the other primitive roots are easier to spot, because they're of the form γ^i for $i \in \{1, 2, \dots, q-1\}$ with $GCD(i, q-1) = 1$:

$$\mathbb{F}_{16}^{\times} = \{1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5, \gamma^6, \gamma^7, \gamma^8, \gamma^9, \gamma^{10}, \gamma^{11}, \gamma^{12}, \gamma^{13}, \gamma^{14}\}$$

	1	γ	γ^2	γ^3	γ^4	γ^5	γ^6	γ^7	γ^8	γ^9	γ^{10}	γ^{11}	γ^{12}	γ^{13}	γ^{14}
order:	1	15	15	5	15	3	5	15	15	5	3	15	5	15	15

primitive elements: $\gamma, \gamma^2, \gamma^4, \gamma^7, \gamma^8, \gamma^{11}, \gamma^{13}, \gamma^{14}$

REMARK: Primitive roots also help us find CRC generator polynomials $g(x)$ in $\mathbb{F}_p[x]$ that catch 2-digit errors that are far apart.

Recall $g(x)$ as a CRC catches such errors up to N digits apart where N is smallest such that $g(x) \mid x^N - 1$ in $\mathbb{F}_p[x]$.

PROPOSITION: Let $(x) \in \mathbb{F}_p[x]$ be irreducible, so that $\mathbb{F}_q = \mathbb{F}_p[x]/(g(x))$ is a field of size $q = p^d$ where $d = \deg(g(x))$.

Then the smallest N for which $g(x) \mid x^N - 1$ is the order of $\alpha := \bar{x}$ in this field $\mathbb{F}_q$.

In particular, N divides $q - 1 = p^d - 1$, with equality $N = p^d - 1 \iff \alpha$ is a primitive root.

In this case, one calls $g(x)$ a primitive (irreducible) polynomial in $\mathbb{F}_p[x]$.

---

proof: $g(x) \mid x^N - 1$ in $\mathbb{F}_p[x]$

$$\iff \bar{x}^N - \bar{1} = \bar{0} \text{ in } \mathbb{F}_p[x]/(g(x)) \; (=: \mathbb{F}_q)$$

$$\iff \bar{1} = \bar{x}^N \; (= \alpha^N)$$

Hence the smallest such N is the order of α ☒

UPSHOT: Primitive polynomials $g(x)$ in $\mathbb{F}_p[x]$ make very good choices for CRC's catching 2-digit errors.

EXAMPLES

(1) In $\mathbb{F}_{16} = \mathbb{F}_2[x]/(\underbrace{x^4+x+1}_{g(x)})$, we checked

$\alpha = \bar{x}$ was a primitive root, so

$g(x) = x^4+x+1$ in $\mathbb{F}_2[x]$ is a primitive polynomial,

and used as a CRC will catch 2-bit errors up to $N = 16-1 = 15$ bits apart.

(2) Garrett (§5.4) mentions $g(x) = x^{15}+x+1 \in \mathbb{F}_2[x]$ as being a primitive polynomial,

so as a CRC it will catch 2-bit errors up to $N = 2^{15}-1 = 32767$ bits apart!