V2a Introduction to Finite Fields

DEFINITION A commutative ring $(R,+,\cdot)$ consists of a set R, together with two operations $+: R\times R \to R$ and $\cdot: R\times R \to R$, such that:

(i) $a+(b+c)=(a+b)+c \quad \forall a,b,c\in R$.

(ii) $a+b=b+a \quad \forall a,b\in R$.

(iii) $\exists 0\in R$ with $0+a=a \quad \forall a\in R$.

(iv) For each $a\in R$, $\exists -a\in R$, such that $a+(-a)=0$.

(v) $a\cdot(b\cdot c)=(a\cdot b)\cdot c \quad \forall a,b,c\in R$.

(vi) $a\cdot b=b\cdot a \quad \forall a,b\in R$.

(vii) $\exists 1\in R$, $1\neq 0$, such that $a\cdot 1=a \quad \forall a\in R$.

(viii) $a\cdot(b+c)=a\cdot b+a\cdot c \quad \forall a,b,c\in R$.

- **NOTATION** We will denote $(R,+,\cdot)$ by R.

- **EXAMPLE** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings.

DEFINITION A field $(F,+,\cdot)$ is a commutative ring with an additional property (ix): $\forall a \in F$ with $a \neq 0$, $\exists a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

- **EXAMPLE** $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}$ is not a field.

DEFINITION A field $(F,+,\cdot)$ is a finite field if F is a finite set; otherwise it is an infinite field. If F is a finite field, its order is $|F|$.

- **EXAMPLE** $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are infinite fields.

- **QUESTIONS** 1) For which integers $n \geq 2$ do finite fields of order n exist?
  2) How does one construct such a field, i.e. what are the field elements, and how are field operations performed?

THE INTEGERS MODULO n

- Let $n \geq 2$. Recall that $\mathbb{Z}_n$ consists of the set of equivalence classes of integers modulo n, $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$, with addition and multiplication done in the natural way: $[a]+[b]=[a+b]$, $[a]\cdot[b]=[a\cdot b]$.

- More simply, we write $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, and perform addition and multiplication modulo n.

- EXAMPLE $\mathbb{Z}_9 = \{0, 1, 2, \ldots, 8\}$. In $\mathbb{Z}_9$, $3+7=1$ and $3\cdot 7 = 3$. More precisely, $3+7 \equiv 1 \pmod 9$ and $3\cdot 7 \equiv 3 \pmod 9$.

- FACT $\mathbb{Z}_n$ is a finite commutative ring.

QUESTION: When is $\mathbb{Z}_n$ a field?

THEOREM $\mathbb{Z}_n$ is a field iff n is prime.

PROOF ($\Leftarrow$) Suppose that n is prime. Let $a \in \mathbb{Z}_n$, $a \neq 0$ (so $1 \leq a \leq n-1$). Since n is prime, $\gcd(a,n)=1$. Hence $\exists s,t \in \mathbb{Z}$ such that $as+nt=1$. Reducing both sides modulo n gives $as \equiv 1 \pmod{n}$. Thus, $a^{-1}=s$, and so $\mathbb{Z}_n$ is a field.

($\Rightarrow$) Suppose that n is composite, say $n=ab$ where $2 \leq a,b \leq n-1$. Now, if a^{-1} exists, say $ac \equiv 1 \pmod{n}$, then $abc \equiv b \pmod{n}$, so $nc \equiv b \pmod{n}$. Thus, $b \equiv 0 \pmod{n}$, so $n \mid b$ which is absurd since $2 \leq b \leq n-1$. Hence, $\mathbb{Z}_n$ is not a field. $\square$

QUESTIONS

- We have established the existence of finite fields of order n, for each prime n.
- What about finite fields of order n, where n is composite?
- In particular, is there a finite field of order 4? 6? 8? 9? 10?

V2b Non-existence of Finite Fields

DEFINITION Let F be a field. The characteristic of F, $\text{char}(F)$, is the smallest positive integer m such that $\underbrace{1+1+\cdots+1}_{m}=0$. If no such m exists, then $\text{char}(F)=0$.

EXAMPLE $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0.
$\mathbb{Z}_p$ (p prime) has characteristic p.

THEOREM If $\text{char}(F)=0$, then F is an infinite field.

PROOF The field elements $1, 1+1, 1+1+1, \ldots$ are distinct, because if $\underbrace{1+1+\cdots+1}_{a}=\underbrace{1+1+\cdots+1}_{b}$ where $a<b$, then $\underbrace{(1+1+\cdots+1)}_{b}-\underbrace{(1+1+\cdots+1)}_{a}=\underbrace{1+1+\cdots+1}_{b-a}=0$, contradicting $\text{char}(F)=0$. □

THEOREM Let F be a field with $\text{char}(F) = m \neq 0$. Then m is prime.

PROOF Suppose m is composite, say $m = ab$ where $2 \leq a, b \leq m-1$.

Let $s = \underbrace{1+1+\cdots+1}_{a}$ and $t = \underbrace{1+1+\cdots+1}_{b}$, and note that $s \neq 0, t \neq 0$.

Then $s \cdot t = \underbrace{(1+1+\cdots+1)}_{a} \cdot \underbrace{(1+1+\cdots+1)}_{b} = \underbrace{1+1+\cdots+1}_{m} = 0$.

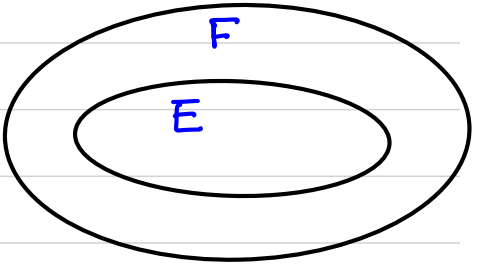
Thus, $s \cdot t \cdot t^{-1} = s \cdot 1 = s = 0$, a contradiction.

We conclude that m is prime. $\square$

SUBFIELDS

- Let F be a finite field of characteristic p.
- Consider the subset of elements of F:

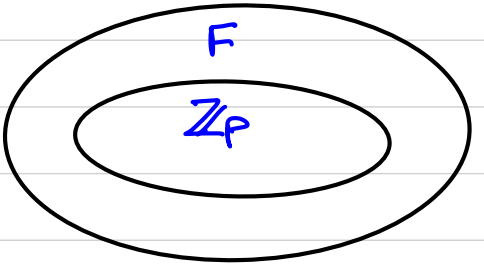
$$E = \{0, 1, 1+1, 1+(1+1), \ldots, \underbrace{1+1+\cdots+1}_{p-1}\}.$$



- The elements of E are distinct.
- One can verify that E is a field, using the same operations as F. E is said to be a subfield of F.
- If we identify the elements of E with the elements of $\mathbb{Z}_p$ in the natural way, then E is essentially the same field as $\mathbb{Z}_p$.
- We have proven:

THEOREM
Let F be a finite field of characteristic p. Then $\mathbb{Z}_p$ is a subfield of F.

FINITE FIELDS AS VECTOR SPACES



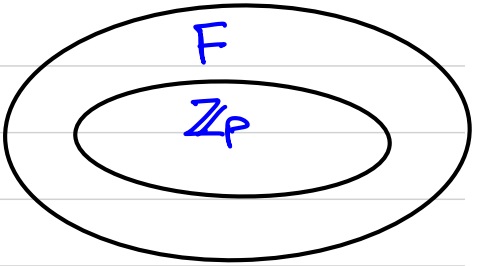
- Let F be a finite field of characteristic p.

- Identify
  - vectors $\longleftrightarrow$ elements of F
  - scalars $\longleftrightarrow$ elements of $\mathbb{Z}_p$
  - vector addition $\longleftrightarrow$ addition of F
  - scalar multiplication $\longleftrightarrow$ multiplication of F.

- Then F is a vector space over $\mathbb{Z}_p$
  (i.e. the axioms that define a vector space are satisfied).

FINITE FIELDS: NON-EXISTENCE

THEOREM Let F be a finite field of characteristic p. Then the order of F is p^n, for some $n \geq 1$.



PROOF Let the dimension of F as a vector space over $\mathbb{Z}_p$ be n. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis for F over $\mathbb{Z}_p$. Then each element $\beta \in F$ can be written uniquely in the form $\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$, where $c_i \in \mathbb{Z}_p$. Thus, $F = \{c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n : c_i \in \mathbb{Z}_p\}$, so $|F| = p^n$. □

EXAMPLE There do not exist finite fields of orders $6, 10, 12, 14, 15, \ldots$.

QUESTION Do finite fields of orders $4, 8, 9, 16, 25, 27, \ldots$ exist?

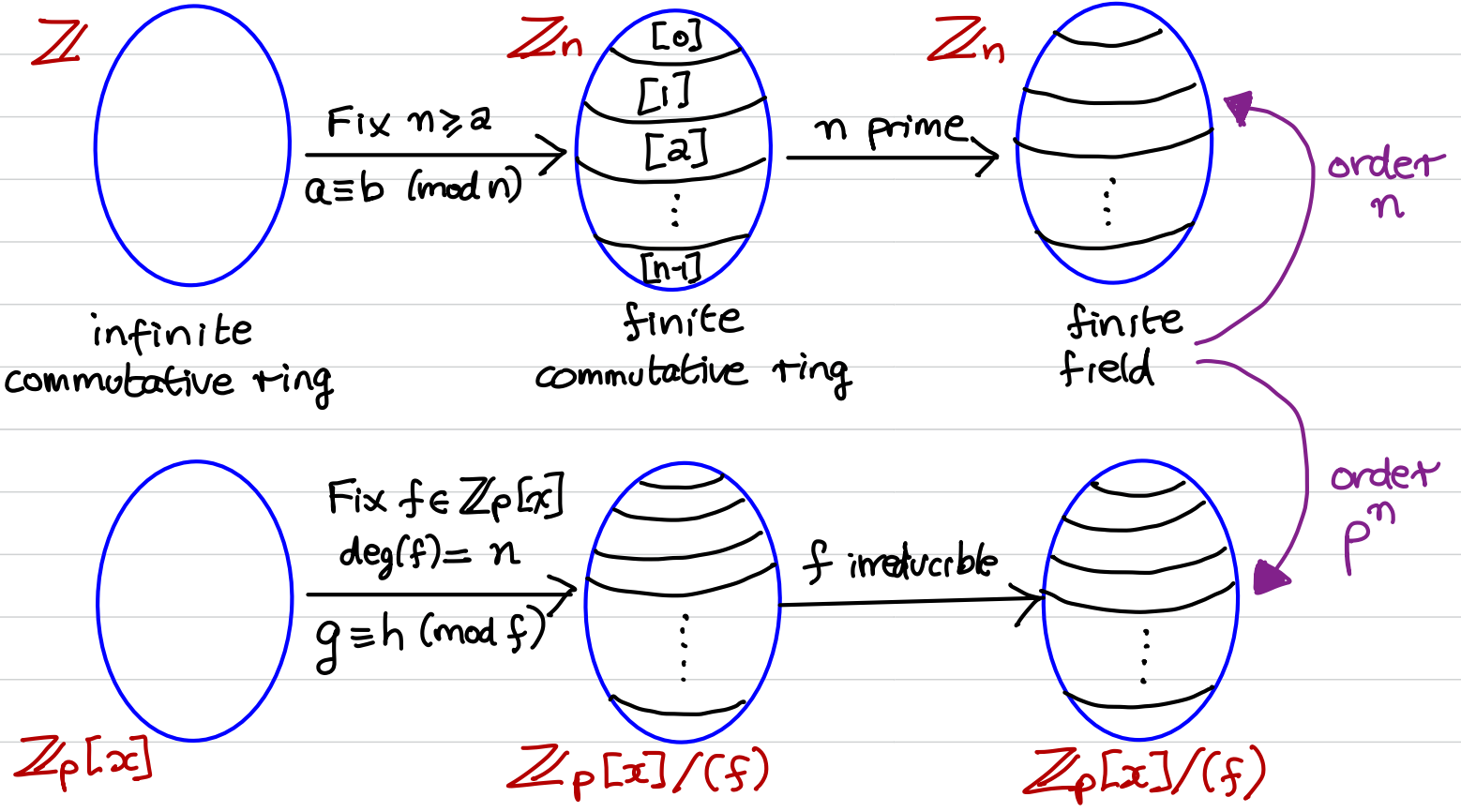
V2c Existence of Finite Fields

- **Polynomial Rings** Let F be a field. Then $F[x]$ denotes the set of all polynomials in x with coefficients from F. Addition and multiplication of polynomials in $F[x]$ is done in the usual way, with coefficient arithmetic done in F.

- **Example** In $\mathbb{Z}_5[x]$,
  - $(3x^4+2x^3+x+4)+(x^5+2x^4+x^2+2x+3) = x^5+2x^3+x^2+3x+2.$
  - $(3x^2+4x+1)\cdot(2x^2+x+2) = x^4+x^3+2x^2+4x+2.$

Fact $F[x]$ is an infinite commutative ring.

CONSTRUCTION OF FINITE FIELDS: MAIN IDEA



POLYNOMIAL DIVISION

- Let $f, g \in F[x]$, with $g \neq 0$. Then there exist unique polynomials $r, s \in F[x]$ with $f = sg + r$ and $\deg(r) < \deg(g)$.

  s: quotient; r: remainder

- By convention, $\deg(0) = -\infty$.

- EXAMPLE Consider $f = 3x^4 + 2x^3 + 2x^2 + x + 1$, $g = 2x^2 + 3x + 4 \in \mathbb{Z}_5[x]$.

$$
\begin{array}{r}
4x^2 + 3 \\
2x^2 + 3x + 4 \overline{)\,3x^4 + 2x^3 + 2x^2 + x + 1} \\
\underline{3x^4 + 2x^3 + x^2} \\
x^2 + x + 1 \\
\underline{x^2 + 4x + 2} \\
2x + 4
\end{array}
$$

quotient: $4x^2 + 3$; divisor: $2x^2 + 3x + 4$; remainder: $2x + 4$

So, $f = (4x^2 + 3)g + (2x + 4)$.

THE RING $F[x]/(f)$

DEFINITION Let $f \in F[x]$ with $\deg(f) \geq 1$. Let $g, h \in F[x]$. Then g is congruent to h modulo f, written $g \equiv h \pmod{f}$, if $g - h = lf$ for some $l \in F[x]$. Equivalently, $f \mid (g-h)$, or g, h leave the same remainder upon division by f.

FACTS The relation $g \equiv h \pmod{f}$ is an equivalence relation and partitions $F[x]$ into equivalence classes: $[g] = \{h \in F[x] : g \equiv h \pmod{f}\}$.
Addition and multiplication is well defined: $[g]+[h] = [g+h]$, $[g]\cdot[h] = [g \cdot h]$.

DEFINITION The set of equivalence classes is denoted $F[x]/(f)$.

THEOREM $F[x]/(f)$ is a commutative ring.

REPRESENTATIVES OF EQUIVALENCE CLASSES OF $F[x]/(f)$

- Suppose that $\deg(f)=n$.
- Let $g \in F[x]$. Long division of g by f yields $g = sf + r$, where $s, r \in F[x]$ with $\deg(r) < n$. Thus $g \equiv r \pmod f$, so $[g] = [r]$.
- Also, if $r_1, r_2 \in F[x]$, $r_1 \neq r_2$, $\deg(r_1) < n$, $\deg(r_2) < n$, then $f \nmid (r_1 - r_2)$, so $r_1 \not\equiv r_2 \pmod f$. Thus $[r_1] \neq [r_2]$.

- Hence, the polynomials in $F[x]$ of degree $< n$ are a complete set of representatives of the equivalence classes of $F[x]/(f)$.

- Now, let $F = \mathbb{Z}_p$. Then $\mathbb{Z}_p[x]/(f) = \{[r] : r \in \mathbb{Z}_p[x], \deg(r) < n\}$
  $= \{[r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}] : r_i \in \mathbb{Z}_p\}$, so $\boxed{|\mathbb{Z}_p[x]/(f)| = p^n.}$

Hence, $\mathbb{Z}_p[x]/(f)$ is a finite commutative ring of order p^n.

- **QUESTION** When is $F[x]/(f)$ a field?

DEFINITION Let $f \in F[x]$ with $\deg(f) \geq 1$. Then f is irreducible over F if f cannot be written as $f = g \cdot h$, $g, h \in F[x]$, $\deg(g) \geq 1$, $\deg(h) \geq 1$.

- **EXAMPLE**
  - x^2+1 is irreducible over $\mathbb{R}$, since it has no roots in $\mathbb{R}$.
  - x^2+1 is reducible over $\mathbb{C}$, since $x^2+1 = (x+i)(x-i)$.
  - x^2+1 is reducible over $\mathbb{Z}_2$, since $x^2+1 = (x+1)(x+1)$.
  - x^2+1 is irreducible over $\mathbb{Z}_3$, since it has no roots in $\mathbb{Z}_3$.

THEOREM $F[x]/(f)$ is a field iff f is irreducible over F.

PROOF Analogous to the proof that $\mathbb{Z}_n$ is a field iff n is prime (see slide 29).

V2d Construction of Finite Fields

Facts about polynomial rings $F[x]$ (F = field)

1) **Factor theorem:** Let $f \in F[x]$ and $c \in F$.
Then $x-c$ is a factor of $f(x)$ iff $f(c)=0$.

2) **Not too many roots:** Let $f \in F[x]$ with $\deg(f)=n \geq 0$.
Then f has at most n roots in F.

3) **Unique factorization** Let $f \in F[x]$ with $\deg(f)=n \geq 0$. Then, up to rearrangement of terms, f has a unique factorization over F:
$f = c f_1^{e_1} f_2^{e_2} \cdots f_t^{e_t}$, where $c \in F$, $f_i \in F[x]$ with f_i monic and irreducible over F, and $e_i \geq 1$.
[A polynomial is monic if its leading coefficient is 1, eg. $f(x)=x^4-3x^2+19$.]

THEOREM Let $f \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $n \geq 1$. Then $\mathbb{Z}_p[x]/(f)$ is a finite field of order p^n and characteristic p. The field elements are the polynomials in $\mathbb{Z}_p[x]$ of degree $< n$.

EXAMPLE (finite field of order $4 = 2^2$) Here, $p=2$ and $n=2$. Let $f(x) = x^2+x+1 \in \mathbb{Z}_2[x]$. Then $f(0)=1$, $f(1)=1$, so f has no roots in $\mathbb{Z}_2$. Thus f is ireducible over $\mathbb{Z}_2$.

So, $F = \mathbb{Z}_2[x]/(x^2+x+1)$ is a finite field of order $2^2=4$.

- The elements of F are $\{0, 1, x, x+1\}$. ([ ] is omitted.)
- Example of addition: $x + (x+1) = 2x+1 = 1$.
- Example of multiplication: $x \cdot (x+1) = x^2 + x = 1$.

EXAMPLE (finite field of order $8 = 2^3$) Here, $p=2$ and $n=3$.
We need an irreducible polynomial of degree 3 over $\mathbb{Z}_2$.
Candidates: x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1.

Try $f(x)=x^3+x+1$. Since $f(0)=1$ and $f(1)=1$, f has no roots in $\mathbb{Z}_2$, and thus no linear factors in $\mathbb{Z}_2[x]$. Thus, f is irreducible over $\mathbb{Z}_2$, and $\boxed{F_1 = \mathbb{Z}_2[x]/(x^3+x+1) \text{ is a finite field of order } 2^3=8.}$

- The elements of F_1 are $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.
- Example of addition: $(x^2+x)+(x^2+x+1)=1$.
- Example of multiplication: $(x^2+x)\cdot(x^2+x+1) = x^4+x = x^2$.
- Example of inversion: $x^{-1}=x^2+1$, since $x\cdot(x^2+1) = x^3+x = 1$.

EXAMPLE (finite field of order $8 = 2^3$) Here, $p=2$ and $n=3$.
$f(x) = x^3+x^2+1$ is irreducible over $\mathbb{Z}_2$, and so

$$F_2 = \mathbb{Z}_2[x]/(x^3+x^2+1) \text{ is a finite field of order } 2^3=8.$$

- The elements of F_2 are $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.

- Note that F_1 and F_2 are <u>not</u> the same field.
  eg. In F_1, $x \cdot x^2 = x+1$, whereas $x \cdot x^2 = x^2+1$ in F_2.

- However, F_1 and F_2 are <u>isomorphic</u> (essentially the same).
  Formally, there is a bijection $\phi: F_1 \longrightarrow F_2$ such that
  $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ $\forall\, a, b \in F_1$.

EXISTENCE AND UNIQUENESS OF FINITE FIELDS

FACT Let p be prime and $n \geq 1$. Then $\exists$ irred. poly. of degree n over $\mathbb{Z}_p$.

THEOREM There exists a finite field of order q iff $q = p^n$ for some prime p and integer $n \geq 1$.

FACT Any two finite fields of the same order are isomorphic.

- We will denote the finite field of order q by $GF(q)$ "the Galois Field of order q".
- In slides 44 and 45, we saw two ways of representing the finite field $GF(2^3)$.

Vae Properties of Finite Fields

THEOREM (Frosh's Dream) Let F be a finite field of characteristic p, and let $\alpha, \beta \in F$. Then $(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$ for all $m \geq 1$.

PROOF ($m=1$) By the Binomial Theorem,

$$(\alpha+\beta)^p = \binom{p}{0}\beta^p + \sum_{i=1}^{p-1}\binom{p}{i}\alpha^i\beta^{p-i} + \binom{p}{p}\alpha^p.$$

Now, for $1 \leq i \leq p-1$, $\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{1\cdot 2\cdot 3\cdots i} \equiv 0 \pmod{p}$, since p divides the numerator but not the denominator, and $\binom{p}{i}$ is an integer.

Thus, $\binom{p}{i}\alpha^i\beta^{p-i} = \underbrace{\alpha^i\beta^{p-i} + \cdots + \alpha^i\beta^{p-i}}_{\binom{p}{i}} = \underbrace{(1+1+\cdots+1)}_{\binom{p}{i}}\alpha^i\beta^{p-i} = 0.$

Hence, $(\alpha+\beta)^p = \alpha^p + \beta^p$. □

THE MULTIPLICATIVE GROUP $GF(q)^*$

DEFINITION The multiplicative group of $GF(q)$ is $GF(q)^* = GF(q) \setminus \{0\}$.

THEOREM Let $\alpha \in GF(q)^*$. Then $\alpha^{q-1} = 1$.

NOTE: If $GF(q) = \mathbb{Z}_p$, then this is Fermat's Little Theorem.

PROOF Let the distinct elements of $GF(q)^*$ be $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$.

Consider the (nonzero) elements $\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_{q-1}$. These elements are distinct because if $\alpha\alpha_i = \alpha\alpha_j$ for some $i \neq j$, then $\alpha^{-1}(\alpha\alpha_i) = \alpha^{-1}(\alpha\alpha_j)$, so $\alpha_i = \alpha_j$, a contradiction.

Hence, $\{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_{q-1}\} = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$, and so

$$(\alpha\alpha_1)(\alpha\alpha_2)\cdots(\alpha\alpha_{q-1}) = \alpha_1\alpha_2\cdots\alpha_{q-1}.$$

Cancelling gives $\alpha^{q-1} = 1$. □

COROLLARY Let $\alpha \in GF(q)$. Then $\alpha^q = \alpha$.

ORDERS OF FIELD ELEMENTS

DEFINITION Let $\alpha \in GF(q)^*$. The order of α, denoted $\text{ord}(\alpha)$, is the smallest positive integer t such that $\alpha^t = 1$.

THEOREM Let $\alpha \in GF(q)^*$, $\text{ord}(\alpha) = t$. Then $\alpha^s = 1$ iff $t \mid s$.

PROOF Let $s \in \mathbb{Z}$. Then long division of s by t yields

$$s = lt + r, \text{ where } 0 \le r < t.$$

Now, $\alpha^s = \alpha^{lt+r} = (\alpha^t)^l \cdot \alpha^r = \alpha^r$,

Hence, $\alpha^s = 1 \iff \alpha^r = 1 \iff r = 0 \iff t \mid s$. □

COROLLARY Let $\alpha \in GF(q)^*$. Then $\text{ord}(\alpha) \mid (q-1)$.

EXAMPLE There is only one element in $GF(q)$ of order 1, namely $\alpha = 1$.

- **EXAMPLE** Consider $GF(2^3) = \mathbb{Z}_2[x]/(x^3+x+1)$.
  The order of $\alpha = x^2+1$ is 7.

- **EXAMPLE** Consider $GF(2^4) = \mathbb{Z}_2[x]/(x^4+x+1)$.
  $f(x) = x^4+x+1$ has no roots in $\mathbb{Z}_2$, thus no linear factors.
  Also, $f(x)$ has no irreducible quadratic factors since $(x^2+x+1) \nmid f(x)$.
  Hence, f is irreducible over $\mathbb{Z}_2$.

Find $\text{ord}(x)$ in $GF(2^4)$.

SOLUTION We have $x^1 = x$, $x^2 = x^2$, $x^3 = x^3$, $x^4 = x+1$, $x^5 = x^2+x$.
Thus, $\text{ord}(x) \neq 1, 3, 5$. Since $\text{ord}(x) \mid 15$, we must have $\underline{\text{ord}(x) = 15}$.

FACT Let $\alpha \in GF(q)^*$ with $\text{ord}(\alpha)=t$. Then the elements $\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{t-1}$ are distinct. In particular, if $\text{ord}(\alpha)=q-1$, then $\{\alpha^0, \alpha^1, \ldots, \alpha^{q-2}\} = GF(q)^*$.

DEFINITION A generator of $GF(q)^*$ is an element in $GF(q)$ of order $q-1$.

EXAMPLE $\alpha = x$ is a generator of $GF(2^4)^*$, where $GF(2^4) = \mathbb{Z}_2[x]/(x^4+x+1)$.
Let's verify that $\text{ord}(x)=15$.

$x^0=1$, $x^1=x$, $x^2=x^2$, $x^3=x^3$, $x^4=x+1$, $x^5=x^2+x$, $x^6=x^3+x^2$,
$x^7=x^3+x+1$, $x^8=x^2+1$, $x^9=x^3+x$, $x^{10}=x^2+x+1$, $x^{11}=x^3+x^2+x$,
$x^{10}=x^3+x^2+x+1$, $x^{13}=x^3+x^2+1$, $x^{14}=x^3+1$, $x^{15}=1$.

THEOREM $GF(q)^*$ has a generator.

PROOF omitted. □