Facts

- $\gcd(i,t)$ = the greatest common divisor of i and t = the largest positive integer m such that $m|i$ and $m|t$.
  - $b|ax \Rightarrow \frac{b}{\gcd(a,b)}\Big| x$

    Proof. $b|ax \Rightarrow \frac{ax}{b} \in \mathbb{N}$. Let $a = k_1 \gcd(a,b)$, and $b = k_2 \gcd(a,b)$, with $\gcd(k_1,k_2)=1$. Then, $\frac{ax}{b} = \frac{k_1 \gcd(a,b) x}{k_2 \gcd(a,b)} = \frac{k_1 x}{k_2} \in \mathbb{N}$. But $\gcd(k_1,k_2)=1$; hence, $k_2|x$.
- $(q-1)|(q^m-1)$.
- Let p be a prime. Then $\gcd(p^{k_1}, p^{k_2}-1)=1$. Also, if $a|p^{k_2}-1$, $\gcd(p^{k_1}, p^{k_2}-1)=1$.

  Proof. Having p^{k_1} implies gcd = p^{k_0}, $k_0 \le k_1, k_2$. To have $\frac{p^{k_2}-1}{p^{k_0}} = p^{k_2-k_0} - \frac{1}{p^{k_0}} \in \mathbb{N}$, k_0 has to be 0.

  (Remark: To see that $k_0 \le k_2$, note that $p^{k_2} \ge p^{k_2}-1 \ge p^{k_0}$.)
- $a|b$, $a|cd$, $\gcd(b,c)=1 \Rightarrow a|d$.

  Proof. Let $x \ne 1$ be any factor of a. Then $x|a$. This implies $x|b$. Now, if $x|c$, then x is a common divisor of b and c, which contradicts $\gcd(b,c)=1$. So, not factor of a is in c. To have $a|cd$, we must have all factors of a in d.

  Proof. $\gcd(a,b)=1 \Rightarrow \exists\ s,t \in D\ \ sa+tb=1$. $a|(bc) \Rightarrow bc = aq$ for some $q \in D$. $sa+tb=1 \Rightarrow sac+tbc=c \Rightarrow sac+taq=c \Rightarrow a(sc+tq)=c$.
- $p\Big|\binom{p}{k}$ for all $k \in \{1,2,3,\dots,p-1\}$ and for all prime integers p.

  Proof. $\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k(k-1)(k-2)\cdots(2)(1)}$ is always an integer. Since p is prime, none of the integers $k,(k-1),\dots,3,2$ are divisors of p. $\binom{p}{k}$ is thus a multiple of p.

Finite fields / Galois Fields

- Finite fields were discovered by Evariste Galois and are thus known as Galois fields.

- The Galois field of order q is usually denoted GF(q).
- GF(q) is a field. Hence
  1. GF(q) forms a commutative group under +.
     The additive identity element is labeled "0".
  2. $\mathrm{GF}(q)\setminus\{0\}$ forms a commutative group under $\cdot$.
     The multiplicative identity element is labeled "1".
  3. The operation "+" and "$\cdot$" distribute: $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.
- A finite field of order q is unique up to isomorphism.
  - Two finite fields of the same size are always identical up to the labeling of their elements.
  - The order of Galois field completely specifies the field.

- The integers {0, 1, 2, …, p-1}, where p is a prime, form the field GF(p) under modulo p addition and multiplication.

- The **order q of a Galois field** GF(q) must be a power of a prime.
- Finite fields of order p^m where p is a prime can be constructed as vector spaces over the prime order field GF(p).
- It is possible to represent $\mathrm{GF}(q^m)$ as an m-dimensional subspace over $\mathrm{GF}(q)$, where $\mathrm{GF}(q)$ is a subfield of $\mathrm{GF}(q^m)$ of prime power order.

- Because $\mathrm{GF}(p^m)$ contains the prime-order field $\mathrm{GF}(p)$ and can be viewed as construction over $\mathrm{GF}(p)$, we call $\mathrm{GF}(p^m)$ an **extension** of the field of order p.
  - Fields of order 2^m can be referred to as a **binary extension field**.
- $\forall\beta\in\mathrm{GF}(q)$, at some point the sequence $1,\beta,\beta^2,\beta^3,\ldots$ begins to repeat values found earlier in the sequence. The first element to repeat must be 1.

  Proof. (1) GF(q) has only a finite number of elements; hence, the sequence must repeat. (2) Assume $\beta^x=\beta^y\neq 1 \;\; x>y>0$ is the first sequence to repeat. Then, because $\beta^y\beta^{x-y}=\beta^x=\beta^y$, multiply both sides by $(\beta^y)^{-1}$ to get $\beta^{x-y}=1$. So, 1 is repeated before $(0<x-y<x)$ the sequence reaches β^x. Contradiction.

Order and characteristic

- The **order of a Galois Field Element**:

  Let $\beta\in\mathrm{GF}(q)$. $\mathrm{ord}(\beta)$ = the order of β = $\min\limits_{m\in\mathbb{N}}\{m:\beta^m=1\}$
- $\forall\beta\in\mathrm{GF}(q)$, nonzero

- $S = \{\beta, \beta^2, \beta^3, \ldots, \underbrace{\beta^{\text{ord}(\beta)}}_{=1}\} = \{\beta^i : 1 \le i \le t\}$
    - Forms a subgroup of the $\text{GF}(q) \setminus \{0\}$ under multiplication
    - Contains all of the solutions to the expression $x^{\text{ord}(\beta)} = 1$.
- $\text{ord}(\beta) | (q-1)$
- $\beta^s = 1 \Leftrightarrow \text{ord}(\beta) | s$
- $\beta^{q-1} = 1$, i.e., $\beta^q = \beta$.
- Let $\alpha, \beta \in \text{GF}(q)$ such that $\beta = \alpha^i$. Then, $\text{ord}(\beta) = \dfrac{\text{ord}(\alpha)}{\gcd(i, \text{ord}(\alpha))}$.

- The **order of a Galois Field Element**:

  Let $\beta \in \text{GF}(q)$. $\text{ord}(\beta)$ = the order of β = $\min_{m \in \mathbb{N}} \{m : \beta^m = 1\}$

    - Order is defined using the multiplicative operation and not additive operation.
- $\forall \beta \in \text{GF}(q)$, nonzero
    - $S = \{\beta, \beta^2, \beta^3, \ldots, \underbrace{\beta^{\text{ord}(\beta)}}_{=1}\} = \{\beta^i : 1 \le i \le t\}$
        - Consists of $\text{ord}(\beta)$ distinct elements.
        - Forms a subgroup of the $\text{GF}(q) \setminus \{0\}$ under multiplication.

          Proof. Let $t = \text{ord}(\beta)$. Then $\beta^m = \beta^{m \bmod t}$. Let $\beta^x, \beta^y \in S$. Then

          $(\beta^y)^{-1} = \beta^{t-y}$.

          $\beta^x (\beta^y)^{-1} = \beta^x \beta^{t-y} = \beta^{t+x-y} = \beta^{(t+x-y) \bmod t} = \beta^{(x-y) \bmod t}$. Because $0 \le (x-y) \bmod t < t$, we have $\beta^x (\beta^y)^{-1} \in S$.
        - Contains all of the solutions to the expression $x^{\text{ord}(\beta)} = 1$.
    - $\text{ord}(\beta) | (q-1)$.

      Proof. Because $\{\beta, \beta^2, \beta^3, \ldots, \underbrace{\beta^{\text{ord}(\beta)}}_{=1}\}$ is a subgroup of $\text{GF}(q) \setminus \{0\}$, by Lagrange's theorem, $\left|\{\beta, \beta^2, \beta^3, \ldots, \underbrace{\beta^{\text{ord}(\beta)}}_{=1}\}\right|$ divides $|\text{GF}(q) \setminus \{0\}|$.

      Hence, $t | (q-1)$.
        - This determines the possible orders a finite field element can display.
    - $\beta^s = 1 \Leftrightarrow \text{ord}(\beta) | s$.

Proof. "$\Leftarrow$" $\operatorname{ord}(\beta)\,|\,s \Rightarrow s = k\operatorname{ord}(\beta),\ k \in \mathbb{N}\cup\{0\} \Rightarrow$

$$\beta^s = \left(\beta^{\operatorname{ord}(\beta)}\right)^k = 1^k = 1.$$

"$\Rightarrow$" (1) If $s = 0$, then $\operatorname{ord}(\beta)\,|\,0$ trivially. (2) If $s > 0$, then we can write $s = \underset{\in \mathbb{N}\cup\{0\}}{q}\operatorname{ord}(\beta) + \underset{\in\{0,\ldots,\operatorname{ord}(\beta)\}}{r}$, i.e., $r = s \bmod \operatorname{ord}(\beta)$. Note that

$$\beta^s = \beta^r \left(\beta^s = \left(\cancel{\beta^{\operatorname{ord}\beta}}^{\,1}\right)^q \beta^r = \beta^r \right).$$ So, $\beta^s = \beta^r = 1$. From $\beta^r = 1$, we

know that r must then be 0; otherwise, contradict the minimality of the order of β.

- $\beta^{q-1} = 1$, i.e., $\beta^q = \beta$.

  Proof. $\operatorname{ord}(\beta)\,|\,(q-1)$.

- Let $\alpha, \beta \in \mathrm{GF}(q)$ such that $\beta = \alpha^i$. Then, $\operatorname{ord}(\beta) = \dfrac{\operatorname{ord}(\alpha)}{\gcd(i, \operatorname{ord}(\alpha))}$.

  Proof. Let $\operatorname{ord}(\alpha) = t$, and $\operatorname{ord}(\beta) = x$. Note that $\dfrac{t}{\gcd(i,t)}, \dfrac{i}{\gcd(i,t)} \in \mathbb{N}$; hence

  $$\beta^{\frac{t}{\gcd(i,t)}} = \left(\alpha^i\right)^{\frac{t}{\gcd(i,t)}} = \left(\alpha^t\right)^{\frac{i}{\gcd(i,t)}} = 1^{\frac{i}{\gcd(i,t)}} = 1.$$ This implies

  $\operatorname{ord}(\beta)\,\Big|\,\dfrac{t}{\gcd(i,t)}$, i.e., $x\,\Big|\,\dfrac{t}{\gcd(i,t)}$. Similarly, since $1 = \beta^{\operatorname{ord}(\beta)} = \left(\alpha^i\right)^x$, we have $\operatorname{ord}(\alpha)\,|\,ix$, i.e., $t\,|\,ix$ which implies $\dfrac{t}{\gcd(i,t)}\,\Big|\,x$. Because we have $x\,\Big|\,\dfrac{t}{\gcd(i,t)}$ and $\dfrac{t}{\gcd(i,t)}\,\Big|\,x$. Hence, $x = \dfrac{t}{\gcd(i,t)}$.

- $\operatorname{ord}(\alpha^i) = \operatorname{ord}(\alpha)$ iff $\gcd(i, \operatorname{ord}(\alpha)) = 1$.

  Proof. $\operatorname{ord}(\alpha^i) = \dfrac{\operatorname{ord}(\alpha)}{\gcd(i, \operatorname{ord}(\alpha))}$.

- An element with order (q-1) in $\mathrm{GF}(q)$ is called a **primitive element** in $\mathrm{GF}(q)$.
  Every field $\mathrm{GF}(q)$ contains exactly $\phi(q-1) \geq 1$ primitive elements.

- The **Euler ϕ function**: $\phi(t) = \left|\{1 \leq i < t \,|\, \gcd(i,t) = 1\}\right| = t \displaystyle\prod_{\substack{\text{prime number } p \\ 1<p<t \\ p|t}} \left(1 - \frac{1}{p}\right)$

- $\phi\left(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}\right) = p_1^{a_1-1}\left(p_1-1\right) p_2^{a_2-1}\left(p_2-1\right)\cdots p_n^{a_n-1}\left(p_n-1\right)$

- An element with order (q-1) in $\mathrm{GF}(q)$ is called a **primitive element** in $\mathrm{GF}(q)$.
  - Every field $\mathrm{GF}(q)$ contains exactly $\phi(q-1) \geq 1$ primitive elements.
- The **Euler ϕ function** (**Euler totient function**) evaluated at an integer t = $\phi(t)$

  = the number of integers in the set $\{1,\ldots,t-1\}$ that are relatively prime to t (i.e., share no common divisors other than one.)

  = $\left|\left\{1 \leq i < t \middle| \gcd(i,t) = 1\right\}\right|$

  = $t \prod_{\substack{\text{prime number } p \\ 1<p<t \\ p|t}} \left(1-\frac{1}{p}\right)$; $\phi(1) = 1$.

  - > 0 for positive t.
  - If p is a prime, then
    - $\phi(p) = p-1$.
    - $\phi(p^m) = p^{m-1}(p-1)$
  - If p_1 and p_2 are distinct prime, then
    - $\phi(p_1 \cdot p_2) = \phi(p_1)\phi(p_2) = (p_1-1)(p_2-1)$
    - $\phi(p_1^m p_2^n) = p_1^{m-1} p_2^{n-1}(p_1-1)(p_2-1)$
  - $\phi\left(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}\right) = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)$

    $= p_1^{a_1-1}\left(p_1-1\right) p_2^{a_2-1}\left(p_2-1\right)\cdots p_n^{a_n-1}\left(p_n-1\right)$
- Given that the integer t divides (q-1), then the number of elements of order t in $\mathrm{GF}(q)$ is $\phi(t)$.

- **The multiplicative structure of Galois Fields**.

  Consider the Galois field $\mathrm{GF}(q)$

  (1) If t does not divide (q-1), then there are no elements of order t in $\mathrm{GF}(q)$.

  (2) If $t|(q-1)$, then there are $\phi(t)$ elements of order t in $\mathrm{GF}(q)$.

  Proof. (2) If $t = \mathrm{ord}(\alpha)$, then the set $\{\alpha, \alpha^2, \ldots, \alpha^t\}$ contains t distinct solutions of $x^t = 1$, and hence the set contains all the solutions. Therefore, all element of order t must contain in this set. To find which one has order t, we know that $\mathrm{ord}(\alpha^i) = \mathrm{ord}(\alpha)$ iff $\gcd(i, \mathrm{ord}(\alpha))$ = 1. Hence, we the number of element with order t is $\left|\left\{1 \le i < t \,\middle|\, \gcd(i,t)=1\right\}\right| = \phi(t)$ by definition.

- $t \mid (q-1)$ iff $\exists \beta \in \mathrm{GF}(q)$ such that $\mathrm{ord}(\beta)=t$.

- In every field $\mathrm{GF}(q)$, there are exactly $\phi(q-1)$ primitive elements.

- $\mathrm{GF}(q)$ can be represented using 0 and (q-1) consecutive powers of a primitive field element $\alpha \in \mathrm{GF}(q)$.
  - All nonzero elements in $\mathrm{GF}(q)$ can be represented as (q-1) consecutive powers of a primitive element α.. Ex. $\left\{\alpha,\alpha^2,\ldots,\underbrace{\alpha^{q-1}}_{1}\right\}$ or $\left\{1,\alpha^2,\ldots,\alpha^{q-2}\right\}$.
  - For $\beta_1,\beta_2 \in \mathrm{GF}(q)\setminus\{0\}$, $\exists i_1,i_2$ such that $\beta_1=\alpha^{i_1}$ and $\beta_2=\alpha^{i_2}$; hence, $\beta_1\cdot\beta_2=\alpha^{i_1}\cdot\alpha^{i_2}=\alpha^{i_1+i_2}=\alpha^{i_1+i_2 \text{ modulo } (q\text{-}1)}$.

  - Note also that $\mathrm{ord}\left(\alpha^i\right)=\dfrac{\mathrm{ord}(\alpha)}{\gcd(i,\mathrm{ord}(\alpha))}=\dfrac{q-1}{\gcd(i,q-1)}$.

  - Multiplication in a Galois field of nonprime order can be performed by representing the elements as powers of the primitive field element α and adding their exponents modulo (q-1).

- Let ***m*(1)** refer to the summation of m ones, i.e., $\underbrace{1\oplus 1\oplus\cdots\oplus 1}_{m\ 1\text{'s}}$.

- Consider the sequence $\left(n(1)\right)_{n=0}^{\infty}=0,1,1\oplus 1,1\oplus 1\oplus 1,\ldots$. Then, 0 is the first repeated elements.

- If $a,b \in \mathrm{GF}(q)$, $a\cdot b=0$, then either a or b must equal zero. Otherwise, $\mathrm{GF}(q)-\{0\}$ cannot form a commutative group under "$\cdot$" because it has no 0.

- The **characteristic** of a Galois field $\mathrm{GF}(q)$ is the smallest positive integer m such that $m(1)=\underbrace{1\oplus 1\oplus\cdots\oplus 1}_{m\ 1\text{'s}}=0$.
  - $\mathrm{GF}\left(p^m\right)$ has characteristic p, where p is a prime number.
  - If $p \mid \ell$, then $\underbrace{\alpha+\alpha+\cdots+\alpha}_{\ell \text{ times}}=0$.

- The **characteristic** of a Galois field $\mathrm{GF}(q)$ is the smallest positive integer m such that $m(1)=\underbrace{1\oplus 1\oplus\cdots\oplus 1}_{m\ 1\text{'s}}=0$.

  - Consider sequence $0,\underbrace{1}_{1(1)},\underbrace{1+1}_{2(1)},\underbrace{1+1+1}_{3(1)},\underbrace{1+1+1+1}_{4(1)},\ldots$

This sequence must begin to repeat and the first element to repeat is 0.

Proof. Since the field is finite, this sequence must begin to repeat at some point. If $j(1)$ is the first repeated element, being equal to $k(1)$ for $0 \le k < j$, it follows that *k* must be zero; otherwise $(j-k)(1)=0$ is an earlier repetition than $j(1)$.

- $m_1(1)\cdot m_2(1)=(m_1m_2)(1)$
- Always a prime integer.

  Proof. Suppose not. Consider the sequence 0, 1, 2(1), 3(1), …, *k*(1), (*k*+1)(1),… Suppose that the first repeated element is *k*(1) = 0 where *k* is not a prime. Then $\exists\ m,n>1$ such that $mn=k$. It follows that $m(1)\cdot n(1)=k(1)$. So we have $m(1)\cdot n(1)=0$, which implies $m(1)=0$ or $n(1)=0$. Since $0<m,n<k$, this contradicts the minimality of the characteristic of the field.

- <u>**Notational caution**</u>: we may write $k(\alpha)$ or $k\alpha$ where $k\in\mathbb{N}$ to denote $\underbrace{\alpha+\alpha+\cdots+\alpha}_{k\text{ times}}$. Note that *k* is irrelevant to the field $\mathrm{GF}(q)$ which contains *α*.. Think of *k* as $k(1)$. Don't confuse this with $\alpha\beta$ or $\alpha\cdot\beta$ where both $\alpha,\beta\in\mathrm{GF}(q)$.
- For a field $\mathrm{GF}(q)$ with characteristic *p*, let $\alpha\in\mathrm{GF}(q)$. Then

  Proof. $\underbrace{\alpha+\alpha+\cdots+\alpha}_{p\text{ times}}=\left(\underbrace{1+1+\cdots+1}_{p\text{ times}}\right)\cdot\alpha=0\cdot\alpha=0$.

  - If $p\,|\,\ell$, then $\underbrace{\alpha+\alpha+\cdots+\alpha}_{\ell\text{ times}}=0$.

- Let GF(*q*) be a (any) field of characteristic *p*, then it contains a **prime-order subfield** GF(*p*) = $Z_p=\{0,1,2(1),3(1),\ldots,(p-1)(1)\}$.

  Proof. The set $Z_p=\{0,1,2(1),3(1),\ldots,(p-1)(1)\}$ contains *p* distinct elements because *p* is the characteristic of GF(*q*) and 0 have to be the first element to repeat. The identities $0,1\in Z_p$. Z_p is closed under both GF(*q*) addition and multiplication because the sum or product of sums of ones is still a sum of ones and $m(1)=(m \bmod p)(1)$. The additive inverse of $j(1)\in Z_p$ is clearly $(p-j)(1)\in Z_p$. The multiplicative inverse of $j(1)$ ($j\ne 0$ or a multiple of *p*) is simply $k(1)$, where $j\cdot k\equiv 1 \bmod p$. *k* exists because we know that $1\in Z_p$ and the set $\{j\cdot x\,|\,x\in Z_p\}=Z_p$ by multiplicative closure and that for $a\ne 0$, $b_1\ne b_2\Rightarrow a\cdot b_1\ne a\cdot b_2$. The rest of the field requirements (Associativity, Distributivity, etc.) are satisfied by noting that Z_p is embedded in the field GF(*q*). $Z_p\subset\mathrm{GF}(q)$ and it is a field.

- Z_p is a subfield of all fields GF(q) of characteristic p.
- Because the field of order p is unique up to isomorphisms,
  Z_p must be the field of integers under modulo p addition and multiplication.

- $\mathrm{GF}\left(p^m\right)$ is an m-dimensional vector space over a field $\mathrm{GF}(p)$.

- Let GF(q) be a (any) field of characteristic p, then it contains a **prime-order subfield** GF(p) = $Z_p = \{0,1,2(1),3(1),\ldots,(p-1)(1)\}$.
- $\mathrm{GF}\left(p^m\right)$, where p is a prime number.
  - is an m-dimensional vector space over a field $\mathrm{GF}(p)$.
  - contains all Galois fields of order p^b where $b|m$.
  - has characteristic p

- The order q of $\mathrm{GF}(q)$ must be a power of a prime.

  Proof. Let β_1 be a nonzero element in GF(q). There are p distinct elements of the form $\alpha_1\beta_1 \in \mathrm{GF}(q)$, where α_1 ranges over all p of the elements in $\mathrm{GF}(p)$.

  (Recall, that $ac = bc$, $c \neq 0 \Rightarrow (a-b)c = 0 \Rightarrow a-b=0 \Rightarrow a=b$)

  If the field $\mathrm{GF}(q)$ contains no other elements, then the proof is complete.

  If there is an element β_2 that is not of the form $\alpha_1\beta_1$, $\alpha_1 \in \mathrm{GF}(p)$, then there are p^2 distinct elements in $\mathrm{GF}(q)$ of the form $\alpha_1\beta_1 + \alpha_2\beta_2 \in \mathrm{GF}(q)$, where $\alpha_1, \alpha_2 \in \mathrm{GF}(p)$.

  This process continues until all elements in $\mathrm{GF}(q)$ can be represented in the form $\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_m\beta_m \in \mathrm{GF}(q)$.

  - Each combination of coefficients $(\alpha_1, \alpha_2, \ldots, \alpha_m) \in (\mathrm{GF}(p))^m$ corresponds by construction to a distinct element in $\mathrm{GF}(q)$.

    Proof. Assume $\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_m\beta_m = \alpha_1'\beta_1 + \alpha_2'\beta_2 + \cdots + \alpha_m'\beta_m$, then we have $\gamma_1\beta_1 + \gamma_2\beta_2 + \cdots + \gamma_m\beta_m = 0$ where $\gamma_i = \alpha_i - \alpha_i'$, not all zero. Let $k = \max_i \{i : \gamma_i \neq 0\}$. Then we have

    $$\beta_k = \left(-\gamma_k^{-1}\gamma_1\right)\beta_1 + \left(-\gamma_k^{-1}\gamma_2\right)\beta_2 + \cdots + \left(-\gamma_k^{-1}\gamma_{k-1}\right)\beta_{k-1}.$$

    Also, $\forall i \ -\gamma_k^{-1}\gamma_i \in \mathrm{GF}(p)$. This contradict the definition of β_k (by construction) because β_k should not be of the form $\beta_k = \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_{k-1}\beta_{k-1}$ where $\alpha_i \in \mathrm{GF}(p)$.

- $\mathrm{GF}(p^m)$ contains all Galois fields of order p^b where $b|m$.

$$\mathrm{GF}(2^6)$$
$$\mathrm{GF}(2^3) \subset \mathrm{GF}(2^6) \supset \mathrm{GF}(2^2)$$
$$\mathrm{GF}(2^3) \supset \mathrm{GF}(2^1) \subset \mathrm{GF}(2^2)$$

  - Need to be able to express $p^m = \left(p^b\right)^\ell$.
  - $\mathrm{GF}(4) \not\subset \mathrm{GF}(32)$

- An element β in $\mathrm{GF}(q^m)$ lies in the subfield $\mathrm{GF}(q)$ if and only if $\beta^q = \beta$.

  Proof. "$\Rightarrow$" Let $\beta \in \mathrm{GF}(q) \subset \mathrm{GF}(q^m)$. Then, $\mathrm{ord}(\beta)|(q-1)$ by the multiplicative structure of GF. So, $\beta^{q-1} = 1$, which implies $\beta^q = \beta$. "$\Leftarrow$" Let $\beta^q = \beta$. Then β is a root of $x^q - x = 0$. The q elements of $\mathrm{GF}(q)$ comprise all q roots of $x^q - x = 0$ and the result follow.

- For nonzero elements β in $\mathrm{GF}(q^m)$, the following are equivalent:

  (1) $\beta \in \mathrm{GF}(q)$

  (2) $\beta^{q-1} = 1$

  (3) $\mathrm{ord}(\beta)|(q-1)$

  Proof. "(1) $\Rightarrow$ (3) $\Rightarrow$ (2)" by the multiplicative structure of Galois fields. "(2) $\Rightarrow$ (3)" because in any $\mathrm{GF}(q')$ we have $\beta^{q-1} = 1 \Rightarrow \mathrm{ord}(\beta)|(q-1)$. Finally, (2) $\Rightarrow$ (1) by theorem above.

- β lies in the subfield $\mathrm{GF}(q)$ if and only if $\beta^q = \beta$. For nonzero β, this is equivalent to $\mathrm{ord}(\beta)|(q-1)$.

- Let α be a primitive element in $\mathrm{GF}(q^m)$. Then, all nonzero elements in $\mathrm{GF}(q^m)$ can be represented as α^j for some integer *j*. An element α^j is in the subfield $\mathrm{GF}(q)$ if and only if $j \cdot q \equiv j$ modulo $(q^m - 1)$.

  Proof. $\alpha^j \in \mathrm{GF}(q)$ iff $\left(\alpha^j\right)^q = \alpha^j$. In $\mathrm{GF}(q^m)$, we have $\left(\alpha^j\right)^q = \alpha^{jq \bmod (q^m-1)}$. So, we want $jq \bmod (q^m - 1) = j$.

  - Remark:
    - $0 \in \mathrm{GF}(q)$.

- $1 = \alpha^0 \in \mathrm{GF}(q)$ because $0 \cdot q \equiv 0$ modulo $\left(q^m - 1\right)$.

- This is equivalent to $j(q-1) \equiv 0 \mod \left(q^m - 1\right)$
- It is also equivalent to $j = k\left(\frac{q^m - 1}{q - 1}\right)$ for $k \in I$, $0 \le k < q - 1$.

  Proof. $j(q-1) \equiv 0 \mod \left(q^m - 1\right)$ means that $j(q-1) = \left(q^m - 1\right)k$. Now, $0 \le j < q^m - 1$. $\left(\alpha^j\Big|_{j=q^m-1} = 1 = \alpha^0\right)$. This implies $\frac{0(q-1)}{q^m - 1} \le k < \frac{\left(q^m - 1\right)(q-1)}{q^m - 1}$. So, $0 \le k < q - 1$.

- **Subfield**: $\mathrm{GF}\left(p^m\right)$, where p is a prime number contains all Galois fields of order p^b where $b \mid m$.
- An element β in $\mathrm{GF}\left(q^m\right)$ lies in the subfield $\mathrm{GF}(q)$ if and only if $\beta^q = \beta$. For nonzero β, this is equivalent to $\mathrm{ord}(\beta) \mid (q-1)$.
- Let α be a primitive element in $\mathrm{GF}\left(q^m\right)$. Then, all nonzero elements in $\mathrm{GF}\left(q^m\right)$ can be represented as α^j for some integer *j*. An element α^j is in the subfield $\mathrm{GF}(q)$ if and only if $j \cdot q \equiv j$ modulo $\left(q^m - 1\right)$ which is equivalent to $j = k\left(\frac{q^m - 1}{q - 1}\right)$ for $k \in I$, $0 \le k < q - 1$.
  - $0, 1 \in \mathrm{GF}(q)$
  - Let $\ell = \frac{q^m - 1}{q - 1}$. Then $\mathrm{GF}(q) = \left\{0, \alpha^0, \alpha^\ell, \alpha^{2\ell}, \alpha^{3\ell}, \ldots, \alpha^{(q-2)\ell}\right\}$.
- It is possible to represent $\mathrm{GF}\left(q^m\right)$ as an *m*-dimensional subspace over $\mathrm{GF}(q)$, where $\mathrm{GF}(q)$ is a subfield of $\mathrm{GF}\left(q^m\right)$ of prime power order.
- Let α, β be elements in the field $\mathrm{GF}\left(p^m\right)$. Then $(\alpha + \beta)^{p^r} = \alpha^{p^r} + \beta^{p^r}$ for *r* = 1, 2, 3, …

  Proof. We will prove the statement by induction on *r*.

  $(\alpha + \beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \binom{p}{2}\alpha^{p-2}\beta^2 + \cdots + \beta^p$. Because $p \,\Big|\, \binom{p}{k}$ for $k \in \{1, 2, 3, \ldots, p-1\}$, we know that $\binom{p}{k} = \binom{p}{k}(1) = \left(\underbrace{1 + 1 + \cdots + 1}_{\binom{p}{k}\text{ times}}\right) = 0$ for

$k \in \{1, 2, 3, \ldots, p-1\}$. Hence, $(\alpha+\beta)^p = \alpha^p + \beta^p$. So, the statement is true for r = 1. Now, let the statement true for $r = \ell$. Then, $(\alpha+\beta)^{p^\ell} = \alpha^{p^\ell} + \beta^{p^\ell}$. We then have

$$\begin{aligned}(\alpha+\beta)^{p^{\ell+1}} &= \left((\alpha+\beta)^{p^\ell}\right)^p = \left(\alpha^{p^\ell} + \beta^{p^\ell}\right)^p = \left(\alpha^{p^\ell}\right)^p + \left(\beta^{p^\ell}\right)^p \\ &= \alpha^{p^{\ell+1}} + \beta^{p^{\ell+1}}\end{aligned}$$

- Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be elements in the field $\mathrm{GF}\left(p^m\right)$, then $\left(\alpha_1+\alpha_2+\cdots+\alpha_t\right)^{p^r} = \alpha_1^{p^r} + \alpha_2^{p^r} + \cdots + \alpha_t^{p^r}$ for r = 1, 2, 3, …

Proof. We will prove by induction on t. Note that the statement is true for t = 2. Now let it be true for $t = \ell$. Them we have

$$\begin{aligned}\left(\alpha_1+\alpha_2+\cdots+\alpha_{\ell+1}\right)^{p^r} &= \left(\left(\alpha_1+\alpha_2+\cdots+\alpha_\ell\right)+\alpha_{\ell+1}\right)^{p^r} \\ &= \left(\alpha_1+\alpha_2+\cdots+\alpha_\ell\right)^{p^r} + \alpha_{\ell+1}^{p^r} \\ &= \alpha_1^{p^r} + \alpha_2^{p^r} + \cdots + \alpha_\ell^{p^r} + \alpha_{\ell+1}^{p^r}\end{aligned}$$