Appunti di algebra dei campi

Definizione: un **campo di Galois** $GF(q)$ è un insieme finito di q elementi su cui sono definite:

- un'operazione di prodotto $\cdot$
  - chiusa: $\forall a,b \in GF(q) \;\; a \cdot b \in GF(q)$:
  - per cui esiste l'elemento neutro 1: $\forall a \in GF(q) \;\; a \cdot 1 = a$;
  - per cui esiste sempre l'elemento inverso: $\forall a \in GF(q), a \neq 0 \exists a^{-1} | a \cdot (a^{-1}) = 1$;
  - commutativa $\forall a,b \in GF(q) \;\; a \cdot b = b \cdot a$;
  - associativa $\forall a,b \in GF(q) \;\; a \cdot b \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- un'operazione di somma $+$
  - chiusa: $\forall a,b \in GF(q) \;\; a + b \in GF(q)$;
  - per cui esiste l'elemento neutro 0: $\forall a \in GF(q) \;\; a + 0 = a$;
  - per cui esiste sempre l'elemento opposto: $\forall a \in GF(q) \exists -a | a + (-a) = 0$;
  - commutativa $\forall a,b \in GF(q) \;\; a + b = b + a$;
  - associativa $\forall a,b \in GF(q) \;\; a + b + c = (a + b) + c = a + (b + c)$;
  - distributiva rispetto al prodotto a $\forall a,b,c \in GF(q) \;\; a \cdot (b + c) = a \cdot b + a \cdot c$.

Si dimostra che: $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$.

Si dimostra che: $\nexists k^{-1} \in GF(q) | k^{-1} \cdot 0 = 1$.

Si dimostra che: $\forall a,b,c \in GF(q) \; se \; a \cdot b \neq a \cdot c \wedge a \neq 0 \Rightarrow a \neq c$.

Si dimostra che: è possibile costruire campi di Galois $GF(q)$ se e solo se q è un numero primo oppure una potenza intera di un numero primo.

Si dimostra che: se esiste un campo di Galois con q elementi allora tale campo è unico, ossia tutti gli altri campi di Galois con q elementi differiscono solo per il nome dei simboli.

Si osserva che: analizzare i campi di Galois $GF(q)$ che hanno come elementi i numeri naturali da 0 a $q-1$ non è restrittivo (d'ora in poi tutti i campi di Galois saranno definiti in questo modo).

Si dimostra che: dato un numero primo q si può costruire un campo di Galois $GF(q)$ se:

- la somma è definita come somma tra i numeri naturali modulo q ;
- il prodotto è definito come il prodotto tra numeri naturali modulo q .

Si dimostra, in particolare, che: un campo di Galois definito come al punto precedente ammette un inverso unico $\forall q \neq 0$ **.**

Si dimostra che: è possibile costruire campi di Galois con p^m elementi, con p primo ed $m > 1$, ma la somma e il prodotto non possono essere definiti in maniera diversa dal punto precedente.

Definizione: detto p un numero primo ed $m \in \mathbb{N}, m \geq 2$ un **campo di Galois esteso** $GF(p^m)$ è un campo di Galois i cui p^m elementi sono costituiti da tutte le possibili m-uple distinte degli elementi di $GF(p)$.

- la somma è definita come la somma modulo p termine a termine delle rappresentazioni polinomiali delle m-uple;

- il prodotto è definito come prodotto delle rappresentazioni polinomiali delle m-uple modulo $P(\alpha)$. $P(\alpha)$ è un particolare polinomio detto generatore del campo;

Definizione: **rappresentazione polinomiale** degli elementi in $GF(p^m)$. Ogni m-upla in $GF(p^m)$ può essere rappresentata da un polinomio $q(\alpha)=\alpha^0 p_0+\alpha^1 p_1+...+\alpha^{m-1} p_{m-1}$ dove i coefficienti p_i sono gli elementi della m-upla. $q(\alpha)$ è detta rappresentazione polinomiale della m-upla.

Definizione: il **polinomio generatore** di un campo $GF(p^m)$ è un polinomio di grado m a coefficienti in $GF(p)$ irriducibile.

Si dimostra che: ogni campo di Galois esteso come definito al punto precedente è un campo di Galois.

Si dimostra, in particolare, che: il prodotto è associativo.

Si dimostra, in particolare, che: il campo ammette un inverso $\forall\, q(\alpha)\neq 0$.

Definizione: l'**ordine di un elemento** $q(\alpha)$ in $GF(q)$ è il numero di valori distinti assunti dalle sue potenze intere $q(\alpha)^i, 1\leq i\leq q-1$.

Definizione: un elemento $q(\alpha)$ in $GF(q)$ è **primitivo** se il suo ordine è $q-1$, ossia se le sue potenze assumono tutti i possibili valori del campo tranne 0.

Si dimostra che: ogni campo di Galois esteso ha almeno un elemento primitivo.

Definizione: il **polinomio generatore** di un campo $GF(q)$ è **primitivo** se l'elemento α di quel campo è primitivo (tupla con tutti zeri e un uno in corrispondenza della prima potenza). Nota: il polinomio generatore è parte della definizione del campo, il fatto che α è primitivo o meno dipende anche dalla scelta del polinomio stesso.

Si dimostra che: ogni campo di Galois ha almeno un polinomio generatore primitivo.

Si osserva che: studiare i campi di Galois con polinomio generatore primitivo non è restrittivo (d'ora in poi tutti i campi saranno definiti in questo modo ed α sarà sempre primitivo).

Definizione: **rappresentazione esponenziale** di un elemento del campo esteso $GF(q)$ con polinomio generatore primitivo. Per i punti precedenti, ogni elemento può essere espresso come potenza dell'elemento primitivo α : ogni potenza α^i , con $0\leq i\leq q-2$ è la rappresentazione esponenziale di un elemento.

Si dimostra che: $\alpha^m=\alpha^{(m)modulo(q-1)}$.

Si dimostra che: $\alpha^{q-1}=\alpha^0=1$.

Si dimostra che: $\alpha^m\cdot\alpha^n=\alpha^{(m+n)modulo(q-1)}$.

Si dimostra che: se α ha ordine n allora $\alpha^m=1$ se e solo se m è multiplo di n .

Si dimostra che: se α ha ordine n allora $\alpha^{n+1}=\alpha$.

Si dimostra che: in un campo $GF(q)$ l'ordine di un elemento α^k è $\frac{q-1}{MCD(k,q-1)}$.

Si dimostra che: l'ordine di un elemento è sempre un fattore di $q-1$ (se $q-1$ è primo tutti gli elementi tranne 0 e 1 sono primitivi).

Definizione: logaritmo di Zech $Z(k): 1+\alpha^k=\alpha^{Z(k)}$.

Si dimostra che: $\alpha^n\cdot\alpha^m=\alpha^{n+Z(m-n)}$.

Si dimostra che: se α ha ordine n e β ha ordine m , con n e m coprimi, allora

$\alpha\cdot\beta$ ha ordine nm .

Si dimostra che: $\forall\,\alpha,\beta\in GF(p^m)\ \ (\alpha+\beta)^p=\alpha^p+\beta^p$.

Si dimostra che: $\forall\,\alpha,\beta\in GF(p^m)\ \ (\alpha+\beta)^{p^n}=\alpha^{p^n}+\beta^{p^n}$.

Si dimostra che: $(\sum_{i=0}^{n}\alpha_i)^{p^n}=\sum_{i=0}^{n}\alpha_i^{p^n}$.

Si dimostra che: $\alpha^p=\alpha^{p-1}\cdot\alpha=\alpha\cdot 1=\alpha$.

Si dimostra che: $\alpha^p=\alpha^{p-1}\cdot\alpha=\alpha$.

Si dimostra che: se $f(x)=a_0+a_1x+a_2x^2+\ldots, a_i\in GF(p^m)\,\forall\, i$ allora $(f(\beta))^{p^k}=f(\beta^{p^k})$.

Si dimostra che: se $f(x)=a_0+a_1x+a_2x^2+\ldots, a_i\in GF(p^m)\,\forall\, i$ e β è una radice di f , allora β^{p^k} è radice di f $\forall\, k$.

Definizione: il **polinomio minimo** di $\beta\in GF(p^m)$ è il polinomio di grado minimo con coefficienti in $GF(p)$ che ammette β come radice.

Definizione: la **trasformata di Fourier** di un polinomio $v(x)$ a coefficienti v_i in $GF(q)$ è il polinomio $V(x)$ a coefficienti $V_j=\sum_{i=0}^{N-1}\alpha^{ij}v_i$, dove N è l'ordine di α .

Definizione: l'**antitrasformata di Fourier** di un polinomio $V(x)$ a coefficienti V_j in $GF(q)$ è il polinomio $v(x)$ a coefficienti $v_i=\frac{1}{N}\sum_{j=0}^{N-1}\alpha^{-ij}V_j$.

Si dimostra che: $V_j=v(\alpha^j)$.

Si dimostra che: $v_i=\frac{1}{N}V(\alpha^{-i})$.

Si dimostra che: se e solo se $V_j=0$ allora $v(x)$ ha una radice in α^j .

Si dimostra che: se e solo se $v_i=0$ allora $V(x)$ ha una radice in α^{-i} .

Si dimostra che: la trasformata del prodotto di due sequenze è pari al prodotto di convoluzione circolare tra le sequenze trasformate, ossia se $e_i=f_i g_i$ allora

$E_j=\Im[e_i]=\Im[f_i]*\Im[g_i]=\sum_{k=0}^{N-1}F_k G_{j-k}$, dove $j-k$ si intende modulo N .

Si dimostra che: moltiplicare una sequenza le potenze di α termine a termine equivale a ruotare i coefficienti nella sequenza trasformata, ossia $v_i\alpha^i=\Im^{-1}[V_{j+1}]$. Vale anche la relazione duale $V_j\alpha^{-j}=\Im[v_i+1]$.

Si dimostra che: se nella sequenza V_j d coefficienti ciclicamente consecutivi sono nulli allora la sequenza antitrasformata v_i ha almeno $d+1$ coefficienti non nulli.

Si dimostra che: se v_i in $GF(p)$ $v_{jp^k}=V_j^{p^k}$.