به نام خدا

ضرب به پیمانه m .

مثلاً ضرب به پیمانه 5 ،

$a \otimes b = r$

$a \cdot b = km + r$

$a = 3 , \quad b = 4$

$a \otimes b = 2$

میدانهای متناهی و چندجمله‌ای‌ها

همان طور که اشاره شد اگر p یک عدد اول باشد، مجموعه $\{0, 1, 2, \dots, p-1\}$ با عملیات جمع و ضرب به پیمانه p یک میدان تشکیل می‌دهند. این میدانها را با $GF(p)$ نمایش می‌دهیم و Galois Field می‌نامیم. در این بخش می‌خواهیم میدانهای توسعه یافته بر اساس $GF(p)$ را نیز معرفی کنیم که آنها را با $GF(p^m)$ (m یک عدد صحیح) نمایش می‌دهیم $GF(q)$

بسیاری از کدهای جبری (algebraic) روی چنین میدانهایی تعریف می‌شوند. به همین خاطر برای شناخت این کدها، لازم است مطالبی را در مورد میدانهای اول و میدانهای کول

توسعه یافته، مطرح کنیم.

مشخصه میدان

برای میدان متناهی $GF(q)$، عضو واحد را با '1' نمایش می‌دهیم و حاصلجمع‌های زیر را تشکیل می‌دهیم،

$$\sum_{i=1}^{1} 1 , \quad \sum_{i=1}^{2} 1 , \quad \dots , \quad \underbrace{\sum_{i=1}^{k} 1}_{\underbrace{1+1+\dots+1}_{k\text{ تا}}} , \quad \dots$$

با توجه به اینکه $GF(q)$ نسبت به عملیات جمع بسته است، تمام این حاصلجمع‌ها، در $GF(q)$ قرار دارند. از طرف دیگر چون $GF(q)$ یک میدان متناهی است و دارای تعداد محدودی عضو

است ، بعضی از این حاصلجمع ها ، دارای مقادیر تکراری خواهند بود ، به عبارت دیگر

$$\exists\, m, n \in \mathbb{Z} \;;\; m < n \;;\; \sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1$$

$$\Longrightarrow \sum_{i=1}^{n} 1 - \sum_{i=1}^{m} 1 = 0 \Longrightarrow \sum_{i=1}^{n-m} 1 = 0$$

مشخصه میدان (λ) کوچکترین عددی است که به ازای آن داریم ،

$$\sum_{i=1}^{\lambda} 1 = 0$$

مثال: $GF(2)$ مشخصه میدان $GF(2)$ برابر 2 است زیرا $1+1=0$

مشخصه $GF(p)$ برابر p است زیرا $\sum_{i=1}^{p} 1 = 0$

مشخصه $GF(2^2) \equiv GF(4)$ برابر 2 است زیرا $1+1=0$

(یا می‌توان گفت $GF(4)$ ، $GF(2)$ را در خود دارد به همین جهت مشخصه آن برابر مشخصه $GF(2)$ است)

قضیه: مشخصه هر میدان متناهی $GF(q)$ (λ) یک عدد اول است.

اثبات (برهان خلف) فرض کنیم λ مشخصه میدان یک عدد اول نباشد، در این صورت

می‌توان نوشت $\lambda = km$ $(k, m \neq 1)$

از طرف دیگر می‌دانیم که

$$\sum_{i=1}^{\lambda} 1 = 0$$

$$\xRightarrow{\lambda = km} \sum_{i=1}^{\lambda} 1 = \left(\sum_{i=1}^{k} 1\right)\left(\sum_{j=1}^{m} 1\right) = 0$$

که نتیجه می‌دهد

$$\sum_{i=1}^{k} 1 = 0 \quad \text{یا} \quad \sum_{j=1}^{m} 1 = 0$$

که هیچ‌کدام از موارد بالا نمی‌تواند برقرار باشد، زیرا λ مشخصه میدان است و کوچکترین عددی است که به ازای آن داریم $\sum_{i=1}^{\lambda} = 1 = 0$ و می‌دانیم $m < \lambda$ و $k < \lambda$

قضیه: حاصلجمع‌های $\underbrace{\sum_{i=1}^{1} 1}_{1}, \sum_{i=2}^{2} 1, \dots, \sum_{i=1}^{\lambda} 1 = 0$ متمایز هستند و تشکیل

یک میدان متناهی $GF(\lambda)$ می‌دهند.

با توجه به اینکه تمامی اعضای $GF(\lambda)$ در $GF(q)$ نیز هستند، بنابراین می‌توان گفت

که $GF(\lambda)$ یک زیرمیدان از $GF(q)$ است.

sub_Field

قضیه: اگر $GF(q)$ یک میدان متناهی با مشخصه λ باشد آنگاه، همواره داریم

$$\exists\, m \in \mathbb{Z} \quad ; \quad q = \lambda^{m}$$

مرتبه یک عضو از میدان

میدان متناهی $GF(q)$ را در نظر می‌گیریم و فرض می‌کنیم a یک عضو دلخواه غیرصفر از میدان $GF(q)$ باشد. حاصلضربهای زیر را تشکیل می‌دهیم

$$a,\ \underbrace{a.a}_{a^2},\ \underbrace{a.a.a}_{a^3},\ \dots,\ \underbrace{a.a\dots a}_{k\text{ بار},\ a^k},\ \dots$$

با توجه به اینکه $GF(q)$ نسبت به عملیات ضرب بسته است، تمامی حاصلضربهای بالا عضو $GF(q)$ هستند. از طرف دیگر چون $GF(q)$ یک میدان متناهی است و دارای تعداد اعضای محدودی است، بعضی از حاصلضربهای بالا تکراری خواهند بود، به عبارت دیگر

$$\exists\ m,n \in \mathbb{Z},\ m<n\ ;\quad a^m = a^n$$

$$a^m = a^n \xrightarrow[\text{عضو وارون } a^{-1}]{\text{با توجه به وجود}} a^{n-m} = 1$$

* کوچکترین عدد صحیح n که به ازای آن داشته باشیم $a^n = 1$ ، مرتبه عضو a از میدان $GF(q)$ نامیده می‌شود. $(a \neq 0)$

قضیه: حاصلضرب‌های $a^1, a^2, \dots, a^n = 1$ (n مرتبه عضو دلخواه a از میدان $GF(q)$ است) با عملیات ضرب تشکیل یک گروه آبلی می‌دهند.

ضرب مربوط به میدان

* گروه‌هایی را که تمامی اعضای آن به صورت توانی از یک عضو خاص قابل بیان باشند، گروه دوری (Cyclic) می‌گوییم.

مثال : $GF(3)$ $\{0,1,2\}$

$\times$	1	2
1	1	2
2	2	1

$or(1) = 1$

$or(2) = 2$

قضیه : برای میدان متناهی $GF(q)$ ، برای هر عضو دلخواه غیر صفر a از میدان داریم

$$a^{q-1} = 1$$

اثبات : می‌دانیم که هر میدان متناهی $GF(q)$ دارای q عضو متمایز است. این اعضا را به صورت $b_0, b_1, \dots, b_{q-1}$ در نظر می‌گیریم. a را یک عضو غیر صفر دلخواه از میدان در نظر می‌گیریم و حاصلضرب‌های زیر را تشکیل می‌دهیم.

$ab_1, \dots, ab_{q-1}$ اعضای $GF(q)$ هستند

که این حاصلضرب‌ها متمایز از یکدیگر هستند. بنابراین می‌توان نوشت.

$$b_1 \dots b_{q-1} = (ab_1)(ab_2)\dots(ab_{q-1}) = a^{q-1} b_1 b_2 \dots b_{q-1}$$

$$\Longrightarrow a^{q-1} = 1$$

قضیه: اگر a یک عضو غیرصفر از میدان $GF(q)$ با مرتبه n باشد، آنگاه $q-1$ بر n بخش‌پذیر است.

اثبات (برهان خلف) فرض کنیم $q-1$ بر n بخش‌پذیر نباشد، در این صورت می‌توان نوشت

$$q-1 = kn + r \quad , \quad r \neq 0 \, , \; r < n$$

از طرف دیگر می‌دانیم که $a^{q-1} = 1$

$$1 = a^{q-1} = a^{(kn+r)} = a^{kn} \cdot a^{r} = \underbrace{(a^{n})}_{1}{}^{k} \, a^{r} = a^{r}$$

$\Rightarrow a^{r} = 1$ که این خلاف فرض است. چون n مرتبه a است

و کوچکترین عددی است که به ازای آن $a^{n}=1$ برقرار است و می‌دانیم $r<n$

تعریف عضو اولیه میدان (Primitive element)

a را عضو اولیه میدان $GF(q)$ می‌گوییم هرگاه مرتبه a، برابر $q-1$ باشد.

نتیجه: توانهای عضو اولیه یک میدان، اعضای غیرصفر آن میدان را می‌سازند.

قضیه: هر میدان $GF(q)$ حداقل یک عضو اولیه دارد.

مثال - $GF(7)$ به صورت زیر بیان می‌شود.

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

K	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$or(1) = 1$ $\qquad$ $or(4) = 3$

$or(2) = 3$ $\qquad$ $or(5) = 6 = q-1$

$or(3) = 6 = q-1$ $\qquad$ $or(6) = 2$

* مرتبه تمامی اعضای میدان $GF(q)$ مقسوم علیه‌های $(q-1)$ هستند.

* عملیات در میدان‌های متناهی و چند جمله‌ای‌ها

عملیات جمع و ضرب در میدان‌های متناهی $GF(q)$ با کمک چند جمله‌ای‌ها انجام می‌شود.

یک چند جمله‌ای $f(x)$ روی میدان $GF(q)$ به صورت زیر تعریف می‌شود،

$$f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n$$

که در آن $f_0, f_1, \dots, f_n$ اعضای $GF(q)$ هستند. یعنی

$$f_i \in GF(q) \quad , \quad i = 0, 1, \dots, n$$

درجه چندجمله‌ای $f(x)$ برابر است با بزرگترین توان x با ضریب غیرصفر

* اگر $f(x) = f_0 \neq 0$ درجه $f(x)$ برابر صفر است.
* اگر $f(x) = f_0 = 0$ درجه $f(x)$ برابر $-\infty$ است.

جمع چندجمله‌ای‌ها

دو چندجمله‌ای $f(x) = f_0 + f_1 x + \dots + f_n x^n$ و $g(x) = g_0 + g_1 x + \dots + g_m x^m$

را در نظر می‌گیریم که در آن $n \geq m$ است. در این صورت حاصل جمع این دو چندجمله‌ای

به صورت زیر خواهد بود،

$$f(x)+g(x) = (f_0+g_0)+(f_1+g_1)x+\cdots+(f_m+g_m)x^m+f_{m+1}x^{m+1}+\cdots+f_n x^n$$

منظور از عملیات جمع، جمع تعریف شده روی میدان است

ضرب دو چندجمله‌ای

$$f(x)\,g(x) = f_0 g_0+(f_0 g_1+f_1 g_0)x+\cdots+(f_0 g_m+f_1 g_{m-1}+\cdots+f_m g_0)x^m$$

$$+f_1 g_m x^{m+1}+\cdots+f_n g_m x^{n+m}$$

عملیات جمع و ضرب تعریف شده روی میدان

تقسیم در چندجمله‌ای

منظور از تقسیم چندجمله‌ای $f(x)$ بر چندجمله‌ای $g(x)$، به دست آوردن $q(x)$ و $r(x)$ به صورتی است که رابطه بالا برقرار باشد و درجه $r(x)$ کوچکتر از درجه $g(x)$ باشد.

$$f(x) = q(x)\,g(x) + r(x)$$

$r(x)$ را باقی‌مانده تقسیم $f(x)$ بر $g(x)$ می‌نامیم. اگر $r(x)=0$ آنگاه می‌گوییم $f(x)$ بر $g(x)$ بخش‌پذیر است. یا $g(x)$ یک فاکتور از $f(x)$ است.

خصوصیات عملیاتهای چندجمله‌ای

۱- جمع دو چندجمله‌ای و ضرب دو چندجمله‌ای دارای خاصیت جابجایی است یعنی

$$a(x)+b(x)=b(x)+a(x) \quad , \quad a(x)\,b(x)=b(x)\,a(x)$$

۲- جمع و ضرب دو چندجمله‌ای دارای خاصیت شرکت‌پذیری است یعنی

$$a(x)+[b(x)+c(x)]=[a(x)+b(x)]+c(x)$$

$$a(x)[b(x)\,c(x)]=[a(x)\,b(x)]\,c(x)$$

۳- ضرب چندجمله‌ای روی جمع چندجمله‌ای‌ها توزیع‌پذیر است

$$a(x)\left[b(x)+c(x)\right] = a(x)b(x)+a(x)c(x)$$

مثال: چندجمله‌ای‌های زیر روی $GF(2)$ تعریف شده‌اند،

$$a(x) = 1+x+x^3+x^5 \quad , \quad b(x) = 1+x^2+x^3+x^4+x^7$$

$$a(x)+b(x) = \overbrace{(1+1)}^{0}+x+x^2+(1+1)x^3+x^4+x^5+x^7 = x+x^2+x^4+x^5+x^7$$

$$a(x).\,b(x) = 1+x+x^2+\overbrace{(1+1+1)}^{1}x^3+\overbrace{(1+1)}^{0}x^4+\overbrace{(1+1+1)}^{1}x^5+\dots+x^{12}$$

$$b(x) \mid a(x)$$

$$1 + x^2 + x^3 + x^4 + x^7 = b(x)$$

$$1 + x + x^3 + x^5 = a(x)$$

$$\begin{array}{l}
x^7 + x^4 + x^3 + x^2 + 1 \\
x^7 + x^5 + x^3 + x^2 \\
\hline
x^5 + x^4 + 1 \\
x^5 + x^3 + x + 1 \\
\hline
x^4 + x^3 + x \quad r(x)
\end{array}$$

$$\begin{array}{|l}
x^5 + x^3 + x + 1 \\
\hline
x^2 + 1 \quad q(x)
\end{array}$$

$$b(x) = q(x)\,a(x) + r(x)$$

* اگر $(x-a)$ یک فاکتور از $f(x)$ باشد آنگاه گوییم a یک ریشه از $f(x)$ است

و داریم $f(a)=0$

* اگر $f(x)$ روی $GF(2)$ تعریف شده باشد، اگر $(x+1)$ یک فاکتور $f(x)$ باشد،

آنگاه $f(1)=0$ یا اگر $f(1)$ برابر صفر باشد $(x+1)$ یک فاکتور $f(x)$ است.