Shahid Beheshti University

رمزنگاری

هادی سلیمانی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی

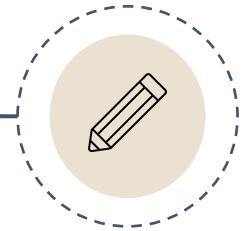
مجوز استفاده و نشر

- اجازه‌ی ایجاد نسخه‌های دیجیتالی جدید براساس بخشی یا تمام مطالب این اسلاید بدون پرداخت هزینه اعطا می‌شود، مشروط بر این‌که:
  - فقط به‌منظور و در راستای استفاده‌ی آموزشی (شخصی و یا کلاسی) ساخته شده باشند و برای کسب هرگونه سود و یا مزیت تجاری استفاده نشوند.
  - نسخه‌های جدید حاوی ارجاع مستقیم به نام تهیه‌کننده اسلاید (هادی سلیمانی) و محل کار وی (پژوهشکده فضای مجازی دانشگاه شهید بهشتی) باشند.
- مجموعه‌ی حاضر براساس نظرات ارزشمند دانشجویان (سابق) دانشگاه شهید بهشتی و همکاران محترم تهیه شده است که از تمام آن‌ها قدردانی می‌شود؛

  (به‌خصوص خانم‌ها **سارا زارعی** و **فاطمه عزیزی** نقش مهمی را در تهیه نسخه‌ی نهایی بر عهده داشته‌اند. خانم مهندس زارعی علاوه بر کمک در آماده‌سازی نسخه‌ی فعلی اسلایدها، در تصحیح اشتباهات نسخه‌ی قبلی و همچنین تکمیل و بازتعریف محتوای درس‌ها بسیار تاثیرگذار بوده‌اند).
- برای مشاهده‌ی اسلایدها و ویدئوهای تدریس این درس به آدرس زیر مراجعه فرمایید:

http://facultymembers.sbu.ac.ir/h_soleimany/cryptography-course/

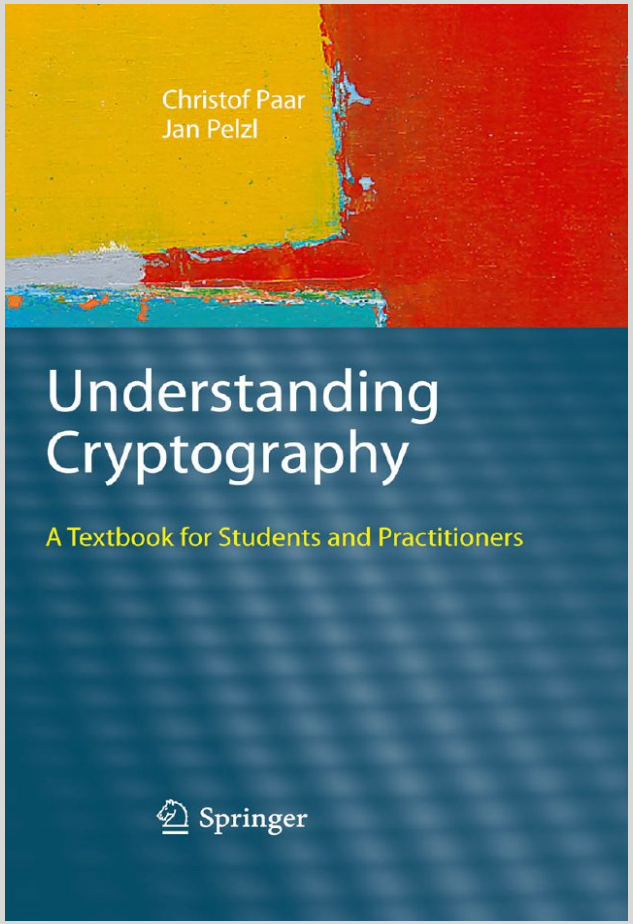
درس یکم



مقدمه‌ای بر ریاضیات رمزنگاری

معرفی مـرجع

مقدمه‌ای بر ریاضیات رمزنگاری



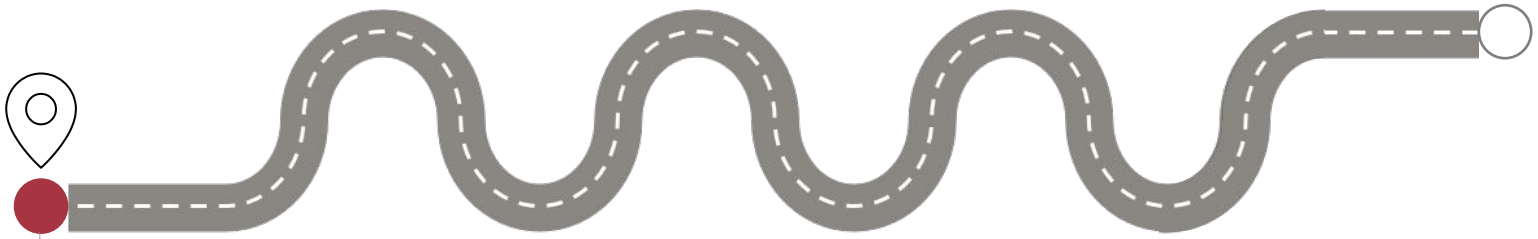
Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

مباحث ریاضیات جبری که در کتاب مرجع در فصل‌های مختلف کتاب و به صورت پراکنده آمده است، در این درس به صورت متمرکز ارائه می‌شود.

فهرست عناوین درس

مقدمه‌ای بر ریاضیات رمزنگاری

- مقدمه
- گروه
- حلقه و میدان
- چندجمله‌ای روی حلقه و میدان
- الگوریتم توسعه‌یافته‌ی اقلیدسی
- ساخت میدان (بزرگ)
- نمایش اعضای میدان
- جمع‌بندی مطالب



مقدمه

چرا به ریاضیات نیاز داریم؟

- علم رمزنگاری به صورت تنگاتنگی با علوم ریاضیات و کامپیوتر در ارتباط است.
- می‌توان گفت که رمزنگاری بر پایه‌ی اصول ریاضیات جبری استوار شده است.
- بنابراین برای ورود به دنیای رمزنگاری و فهم صحیح مطالب لازم است که با یادگیری چند مفهوم پرکاربرد ریاضیات شروع کنیم.
- این درس به این مفاهیم اختصاص دارد و از درس‌های بعد از مباحث محض ریاضیاتی خارج شده و کم‌کم به دنیای شیرین رمزنگاری (ریاضیات کاربردی ؛)) قدم خواهیم گذاشت.

مفاهیم پرکاربرد ریاضیات در رمزنگاری

چندجمله‌ای روی حلقه و میدان، محاسبه‌ی معکوس

ساخت میدان‌های بزرگ

نقش میدان‌ها در تسهیل محاسبات

گروه ، حلقه و میدان

نمایش‌های مختلف اعضای میدان و کاربرد آن‌ها

گروه

مقدمه

گروه

(Group)

- یک گروه، به مجموعه‌ی ناتهی G و یک عملگر دوتایی $*$ گفته می‌شود که در آن خواص زیر برای اعضای مجموعه صادق باشد:

۱- شرکت‌پذیری (Associativity):

$$\forall\, a, b, c \in G: (a * b) * c = a * (b * c)$$

۲- وجود عضو خنثی (همانی) (Identity Element):

$$\exists e \in G: \forall a \in G: a * e = e * a = a$$

۳- وجود عضو قرینه (وارون) (Inverse Element):

$$\forall a \in G, \exists a^{-1} \in G: a * a^{-1} = e$$

۴- بسته بودن (Closure):

$$\forall a, b \in G:\ a * b \in G$$

- تعریف گروه آبلی (Abelian Group): گروه G را آبلی یا جابه‌جایی گوییم هرگاه:

$$\forall a, b \in G: a * b = b * a$$

مثال

- آیا $(\mathbb{Z}, +)$ (مجموعه‌ی اعداد صحیح با عملگر جمع) گروه است؟
  - بله!
  - بسته بودن و شرکت‌پذیری ✓
  - وجود عضو خنثی: $e = 0$ ✓
  - وجود عضو قرینه: $a^{-1} = -a$ ✓
- آیا $(\mathbb{R}, +)$ (مجموعه‌ی اعداد حقیقی با عملگر جمع) گروه است؟
  - بله!
  - بسته بودن و شرکت‌پذیری ✓
  - وجود عضو خنثی: $e = 0$ ✓
  - وجود عضو قرینه: ✓
- آیا $(\mathbb{R}, \times)$ گروه است؟
  - خیر! چون 0 وارون ندارد.
  - بسته بودن و شرکت‌پذیری ✓
  - وجود عضو خنثی: $e = 1$ ✓
  - وجود عضو قرینه: $0^{-1} = ?$
- آیا $(\mathbb{R} - \{0\}, \times)$ گروه است؟
  - بله!
- آیا $(\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}, \times)$ گروه است؟ $(\mathbb{Z}_n = \{0,1,2, \dots, n-1\}$ و منظور از $\times$ در اینجا، ضرب پیمانه‌ای است).
  - نه لزوما! مثلا در $(\mathbb{Z}_4 - \{0\}, \times)$، عضو ۲ وارون ضربی ندارد.

گروه محدود و زیرگروه

(Finite Group & Subgroup)

- گروه محدود (Finite Group): اگر تعداد اعضای گروه محدود باشند، به آن گروه محدود گویند.
- زیرگروه (Subgroup): زیرگروه S از گروه G، زیرمجموعه‌ای از G است که خودش با همان عمل گروه G، تشکیل گروه دهد. در این صورت می‌نویسیم:

$$S < G$$

- مثال: برای گروه $(\mathbb{Z}_4, +)$، $\{0,2\}$ یک زیرگروه است.

مرتبه

(Order)

- مرتبه‌ی گروه: تعداد اعضای یک گروه محدود را مرتبه‌ی گروه گویند و به یکی از صورت‌های زیر نمایش می‌دهند:

$$|G|, \qquad \mathrm{ord}(G), \qquad O(G)$$

  - مثال: مرتبه‌ی گروه $(\mathbb{Z}_5^*, \times)$ برابر است با:

$$\mathbb{Z}_5^* = \{1,2,3,4\} \Rightarrow O(G) = 4$$

- مرتبه‌ی عضو: اگر k کوچکترین عددی باشد که $a^k = e$ باشد، در این صورت k را مرتبه‌ی a می‌نامیم و با $O(a) = k$ نمایش می‌دهیم.
  - مثال: مرتبه عضو 2 در گروه $(\mathbb{Z}_5^*, \times)$ برابر است با:

$$2^4 = 16 = 1 \Rightarrow O(2) = 4$$

  - مثال: مرتبه عضو 1 در گروه $(\mathbb{Z}_5^*, \times)$ برابر است با:

$$1^1 = 1 \Rightarrow O(1) = 1$$

قضیه‌ی لاگرانژ

- فرض کنید G یک گروه متناهی باشد،

الف) مرتبه‌ی هر زیرگروه، مرتبه‌ی گروه را می‌شمارد.

ب) مرتبه‌ی هر عضو، مرتبه‌ی گروه را می‌شمارد.

- مثال اسلاید صفحه قبل: گروه $(\mathbb{Z}_5^*, \times)$ را در نظر بگیرید.

$$\mathbb{Z}_5^* = \{1,2,3,4\} \Rightarrow O(G) = 4$$
$$1^1 = 1 \Rightarrow O(1) = 1 \Rightarrow 1 \mid 4 \ \checkmark$$
$$2^4 = 16 = 1 \Rightarrow O(2) = 4 \Rightarrow 4 \mid 4 \ \checkmark$$

گروه دوری

- اگر G یک گروه باشد و $a \in G$، آنگاه:

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$$

یک زیرگروه G است که زیرگروه دوری تولید شده توسط a نامیده می‌شود.

- گروه G را یک گروه دوری گوییم هرگاه یک عنصر مانند $a \in G$ وجود داشته باشد به‌نحوی‌که: $\langle a \rangle = G$.
- دراین صورت a را مولد G یا ریشه‌ی اولیه در پیمانه n (Primitive root modulo n) می‌گوییم.

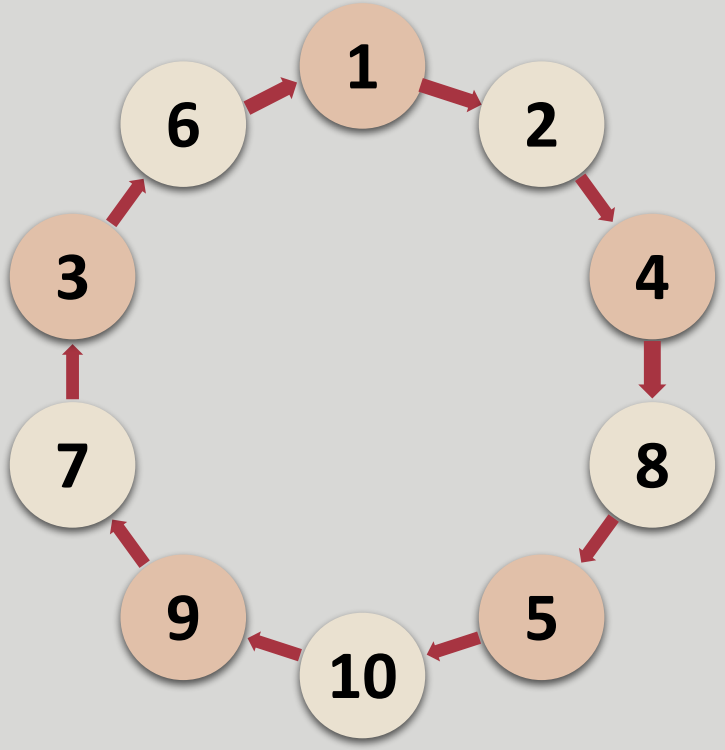
گروه دوری

مثال

- $\mathbb{Z}_{11}^*$ را نسبت به عمل ضرب پیمانه‌ای در نظر می‌گیریم:

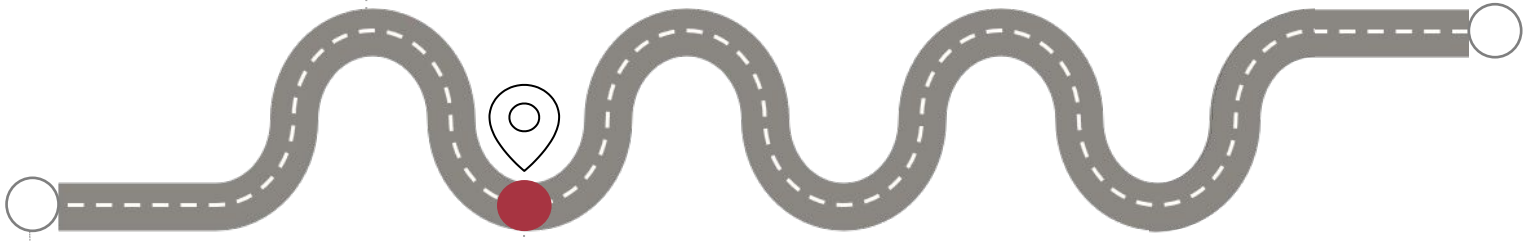
$$\mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\} \quad , \quad \times$$

- بنابراین $a = 2$ مولد گروه $\mathbb{Z}_{11}^*$ است.



$$\langle 2 \rangle = G$$

گروه



مقدمه

حلقه و میدان

حلقه

(Ring)

- یک مجموعه‌ی غیرتهی R با دو عمل $\times$ و $+$، یک حلقه نامیده می‌شود، هرگاه شرایط زیر صادق باشند:

۱- $(R,+)$ یک گروه آبلی باشد.

۲- R نسبت به ضرب شرکت‌پذیر باشد.

$$a,b,c \in R: (a \times b) \times c = a \times (b \times c)$$

۳- R نسبت به دو عمل $\times$ و $+$ از دو طرف توزیع‌پذیر باشد:

$$(a+b) \times c = a \times c + b \times c$$
$$a \times (b+c) = a \times b + a \times c$$

- مثال: $(\mathbb{Z}_n, +, \times)$ حلقه است؟

بله!

میدان

(Field)

- یک مجموعه‌ی غیرتهی F با دو عمل $\times$ و $+$، یک میدان نامیده می‌شود، هرگاه شرایط زیر صادق باشند:

۱- $(F,+)$ یک گروه آبلی باشد.

۲- $(F-\{0\},\times)$ یک گروه آبلی باشد.

۳- F نسبت به دو عمل $\times$ و $+$ از دو طرف توزیع زیر باشد:

$$(a+b)\times c = a\times c + b\times c$$
$$a\times(b+c) = a\times b + a\times c$$

- مثال: $(\mathbb{Z}_6, +, \times)$ میدان است؟

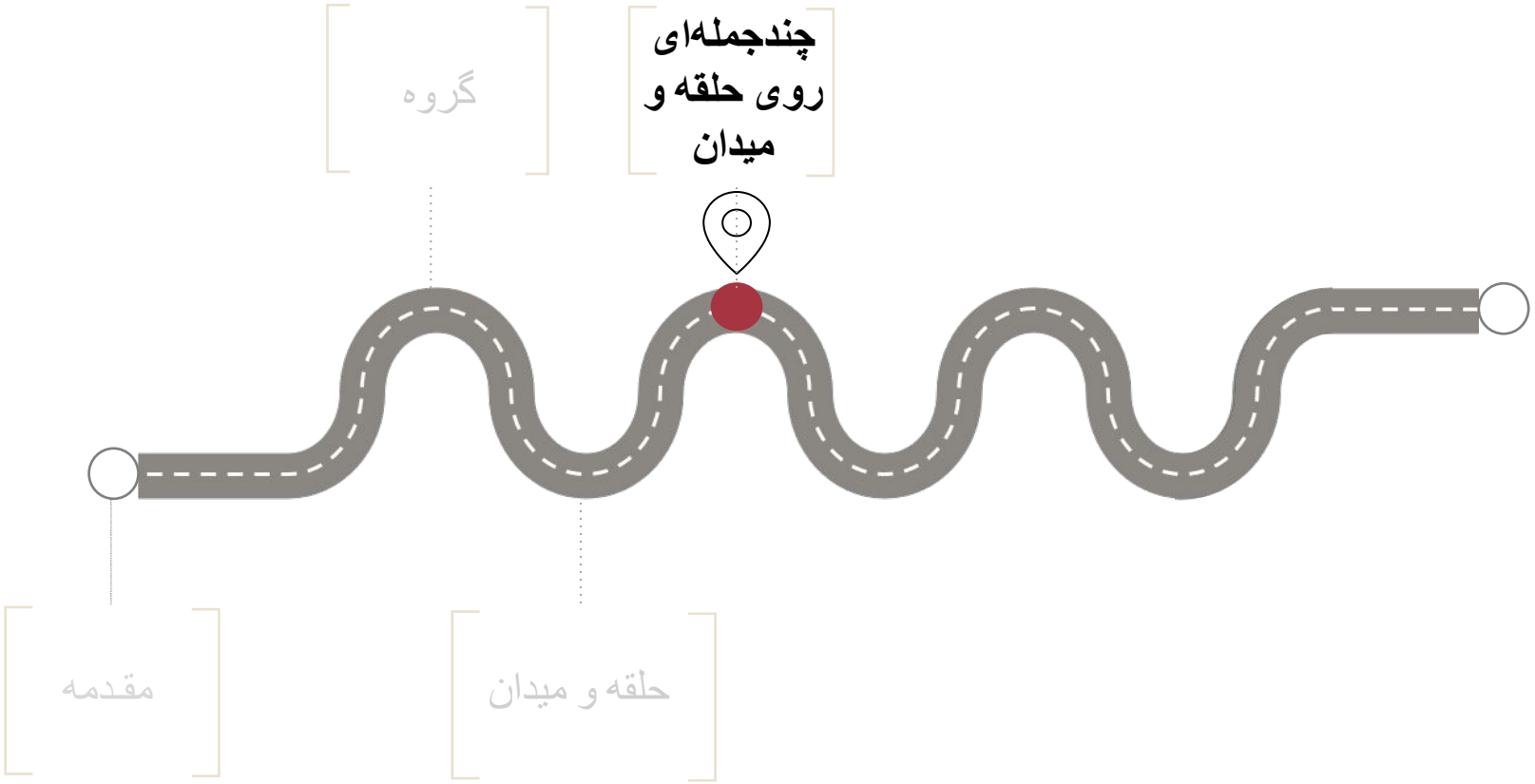
خیر! چون عضو 2 نسبت به عملیات $\times$ معکوس ندارد. اما حلقه است.

- مثال: $(\mathbb{Z}_5, +, \times)$ میدان است؟

بله! تمام اعضای $\{1,2,3,4\}$ نسبت به 5 اول هستند، پس تمام آنها معکوس دارند.

میدان گالوا

- میدان محدود: هرگاه تعداد عناصر میدان F محدود باشد، آن را میدان محدود گوییم (Finite Field).
- میدان گالوا (Galois Field): اگر p یک عدد اول باشد، مجموعه‌ی $\mathbb{Z}_p$ به همراه عملیات‌های $\times$ و $+$ پیمانه‌ای (به پیمانه p) یک میدان تشکیل می‌دهد. این میدان را اصطلاحا میدان گالوا گویند و با $GF(p)$ نمایش می‌دهند.
- دلیل این امر این است که اگر $\gcd(a,n) = 1$، در این صورت a به پیمانه n معکوس دارد.
- اما در حالت کلی، مجموعه‌ی $\mathbb{Z}_n$ به همراه عملیات‌های $\times$ و $+$ پیمانه‌ای (به پیمانه n) یک میدان تشکیل نمی‌دهد.


چندجمله‌ای روی حلقه و میدان
گروه
مقدمه
حلقه و میدان

چندجمله‌ای روی حلقه‌ی R

- فرض کنید که R یک حلقه باشد.

هر عبارت به صورت $f(x) = \sum_{i=0}^{n} a_i x^i$، یک چندجمله‌ای روی حلقه R نامیده می‌شود، درصورتی‌که :

n یک عدد صحیح غیرمنفی و a_iها عضو حلقه R باشند و $a_n \neq 0$.

x نمادی است که (لزوما) به R تعلق نداشته و یک مجهول روی R نامیده می‌شود.

- چندجمله‌ای را می‌توان صرفا با نمایش ضرائب به صورت یک **بردار** نمایش داد:

$$f = (a_0, a_1, \dots, a_n)$$

به a_n ضریب پیشرو (Leading Coefficient) می‌گویند.

- اگر $a_n = 1$ باشد، چندجمله‌ای را تکین (Monic) گویند.
- n نشان‌دهنده‌ی درجه‌ی چندجمله‌ای است که آن را با $\deg(f)$ نمایش می‌دهند.
- نکته: عملیات‌های $\times$ و $+$ بر روی چندجمله‌ای‌های روی یک حلقه قابل اجرا هستند.

چندجمله‌ای روی حلقه‌ی R

مثال

- حلقه‌ی $R = (\mathbb{Z}_6, +, \times)$ و دو چند جمله‌ای زیر را روی آن در نظر بگیرید:

$f(x) = 5x + 4$
$g(x) = 3x^7 + 2x + 2$

- عملیات جمع:

$$f(x) + g(x) = 3x^7 + 7x + 6$$
$$= 3x^7 + x + 0 = 3x^7 + x$$

- عملیات ضرب:

$$f(x) \times g(x) = 15x^8 + 12x^7 + 10x^2 + 8x + 10x + 8$$
$$= 3x^8 + 0x^7 + 4x^2 + 0x + 2$$
$$= 3x^8 + 4x^2 + 2$$

حلقه $R[x]$

- مجموعه‌ی تمامی چندجمله‌ای‌های روی حلقه R را با $R[x]$ نمایش می‌دهیم.
- **قضیه:** اگر R یک حلقه باشد، آنگاه $R[x]$ نیز همراه با اعمال $+$ و $\times$، یک حلقه است و R یک زیرحلقه از $R[x]$ خواهد بود.

حلقه $F[x]$

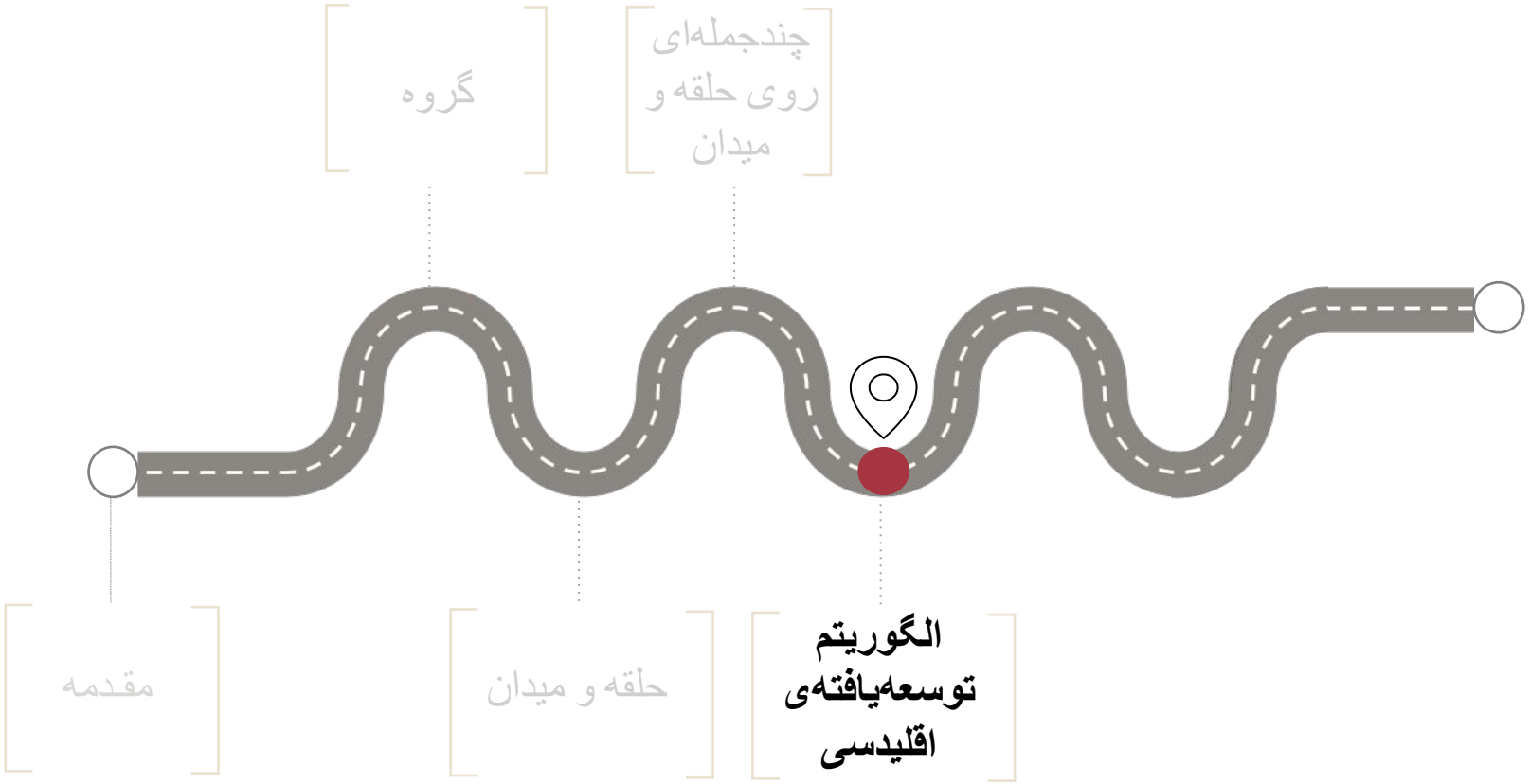
- فرض کنید که F یک میدان باشد.

هر عبارت به صورت $f(x) = \sum_{i=0}^{n} a_i x^i$، یک چندجمله‌ای روی حلقه F نامیده می‌شود، در صورتی که :

n یک عدد صحیح غیرمنفی و a_iها عضو میدان F و $a_n \neq 0$ باشند.

x نمادی است که (لزوما) به F تعلق نداشته و یک مجهول روی F نامیده می‌شود.

- مجموعه‌ی تمامی چندجمله‌ای‌های روی میدان F را با $F[x]$ نمایش می‌دهیم.
- $F[x]$ همراه با اعمال $+$ و $\times$، یک حلقه است.
- توجه: در حالت کلی اعضای $F(x)$ وارون ندارند و در نتیجه $F[x]$ لزوما نمی‌تواند یک میدان باشد.


گروه
چندجمله‌ای روی حلقه و میدان
مقدمه
حلقه و میدان
الگوریتم توسعه‌یافته‌ی اقلیدسی

بزرگ‌ترین مقسوم‌علیه مشترک

(یادآوری)

- **تعریف:** برای اعداد صحیح a و b که حداقل یکی از آن‌ها غیر صفر است، بزرگترین عددی که هر دو عدد را بشمارد، بزرگ‌ترین مقسوم‌علیه مشترک (gcd) می‌نامند.
- **قضیه (الگوریتم تقسیم):** برای اعداد صحیح a و b که $b \neq 0$ است، اعداد صحیح یکتای q و r وجود دارند به نحوی‌که:

$$a = b \times q + r, \qquad 0 \leq r < |b|$$

به r، باقی‌مانده می‌گویند.

الگوریتم اقلیدسی

(یادآوری)

- برای محاسبه‌ی بزرگ‌ترین مقسوم‌علیه مشترک دو عدد $a = 846$ و $b = 208$ به صورت زیر عمل می‌کنیم:

$$r_0 = a = 846\ , r_1 = b = 208$$

- در مرحله‌ی iام برای محاسبه‌ی r_i، باقیمانده r_{i-2} در تقسیم بر r_{i-1} را محاسبه می‌کنیم.

$$r_i = r_{i-2} - q_i r_{i-1}$$

i	q_i	r_i
0	–	846
1	–	208
2	4	14
3	14	12
4	1	2

$$r_2 = 846 - 4 \times 208 = 14$$

$$r_3 = 208 - 14 \times 14 = 12$$

$$r_4 = 14 - 1 \times 12 = 2$$

قضیه Bézout

- برای اعداد صحیح a و b که حداقل یکی از آن‌ها غیر صفر است، اعداد صحیح u و v وجود دارند به نحوی که در رابطه‌ی زیر صدق کنند:

$$u.a + v.b = \gcd(a, b)$$

- می‌توان با توسعه‌ی الگوریتم اقلیدسی و بدون هزینه اضافه، مقادیر u و v را به دست آورد.

الگوریتم توسعه‌یافته‌ی اقلیدسی

- برای محاسبه‌ی بزرگ‌ترین مقسوم‌علیه مشترک دو عدد $a = 846$ و $b = 208$ به صورت زیر عمل می‌کنیم:

$$r_0 = a = 846, r_1 = b = 208$$
$$u_0 = 0, u_1 = 1, v_0 = 1, v_1 = 0$$

- در مرحله‌ی iام مقادیر r_i، u_i و v_i را به صورت زیر محاسبه می‌کنیم.

$$r_i = r_{i-2} - q_i r_{i-1}$$
$$u_i = u_{i-2} - q_i u_{i-1}$$
$$v_i = v_{i-2} - q_i v_{i-1}$$

- می‌توان ثابت کرد که رابطه‌ی زیر در هر مرحله برقرار است:

$$r_i = u_i \times b + v_i \times a$$

i	q_i	r_i	u_i	v_i
0	–	846	0	1
1	–	208	1	0
2	4	14	−4	1
3	14	12	57	−14
4	1	2	−61	15

$$2 = (-61) \times 208 + 15 \times 846$$

کاربرد الگوریتم توسعه‌یافته‌ی اقلیدسی

- برای دو عدد صحیح دلخواه a و b، الگوریتم توسعه‌یافته‌ی اقلیدسی می‌تواند مقادیر u و v را به‌نحوی پیدا کند که رابطه‌ی $d = u \times a + v \times b$ صادق باشد.
- اگر a و b نسبت به یکدیگر اول باشند، داریم:

$$1 = u \times a + v \times b$$

- اگر تساوی فوق را در پیمانه‌ی b محاسبه کنیم، داریم:

$$1 \equiv u \times a \mod b$$

به عبارتی، به کمک این الگوریتم می‌توان معکوس a را در پیمانه‌ی b محاسبه کرد.

- معکوس b در پیمانه a را نیز می‌توان به طور مشابه محاسبه کرد.

الگوریتم تقسیم

کاربرد در چندجمله‌ای‌های عضو $F[x]$

- **قضیه:** اگر F یک میدان و $f,g \in F[x]$ باشند، که g یک چندجمله‌ای غیرصفر است، در این صورت $r,q \in F[x]$ وجود دارند به‌نحوی‌که:

$$f = g \times q + r \quad , \quad \deg(r) < \deg(g)$$

- **مثال:** میدان $GF(5)$ را در نظر بگیرید.

$$\begin{array}{l|l} 3x^5 + 2x^3 + x + 1 & x^3 + 1 \\ \hline 3x^5 + 3x^2 & 3x^2 + 2 \\ \hline 2x^3 + 2x^2 + x + 1 & \\ 2x^3 + 2 & \\ \hline 2x^2 + x + 4 & \end{array}$$

- **تعریف:** اگر $r = 0$ باشد، گوییم چندجمله‌ای g چندجمله‌ای f را می‌شمارد.

بزرگ‌ترین مقسوم‌علیه مشترک

تعریف برای چندجمله‌ای‌های عضو $F[x]$

- **قضیه:** اگر $f,g \in F[x]$ باشند و حداقل یکی از آنها غیرصفر باشد، در این صورت می‌توان نشان داد که چندجمله‌ای تکین $d \in F[x]$ به صورت یکتا وجود دارد، به‌صورتی‌که:

1. $d|f, d|g$
2. If $h \in F[x], h|f, h|g \Rightarrow h|d$
3. $\exists u, v \in F[x]: \; d = uf + vg$

- **تعریف:** d را بزرگ‌ترین مقسوم‌علیه مشترک f و g می‌نامیم و با $\gcd(f,g)$ نمایش می‌دهیم.
- **تعریف:** اگر $d = 1$ باشد می‌گوییم f و g نسبت به هم اول هستند.
- می‌توان مقادیر d، u و v را با استفاده از الگوریتم توسعه یافته اقلیدسی محاسبه کرد.

مثال

- دو چندجمله‌ای $g = x^2$ و $f = x^4 + x + 1$ را در نظر بگیرید که $f, g \in GF(2)[x]$.

i	q_i	r_i	u_i	v_i
0	–	$x^4 + x + 1$	0	1
1	–	x^2	1	0
2	x^2	$x + 1$	x^2	1
3	$x+1$	1	$x^3 + x^2 + 1$	$x + 1$

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

محاسبه‌ی معکوس

- براساس رابطه‌ی به‌دست‌آمده می‌توان معکوس g در پیمانه f را محاسبه کرد.

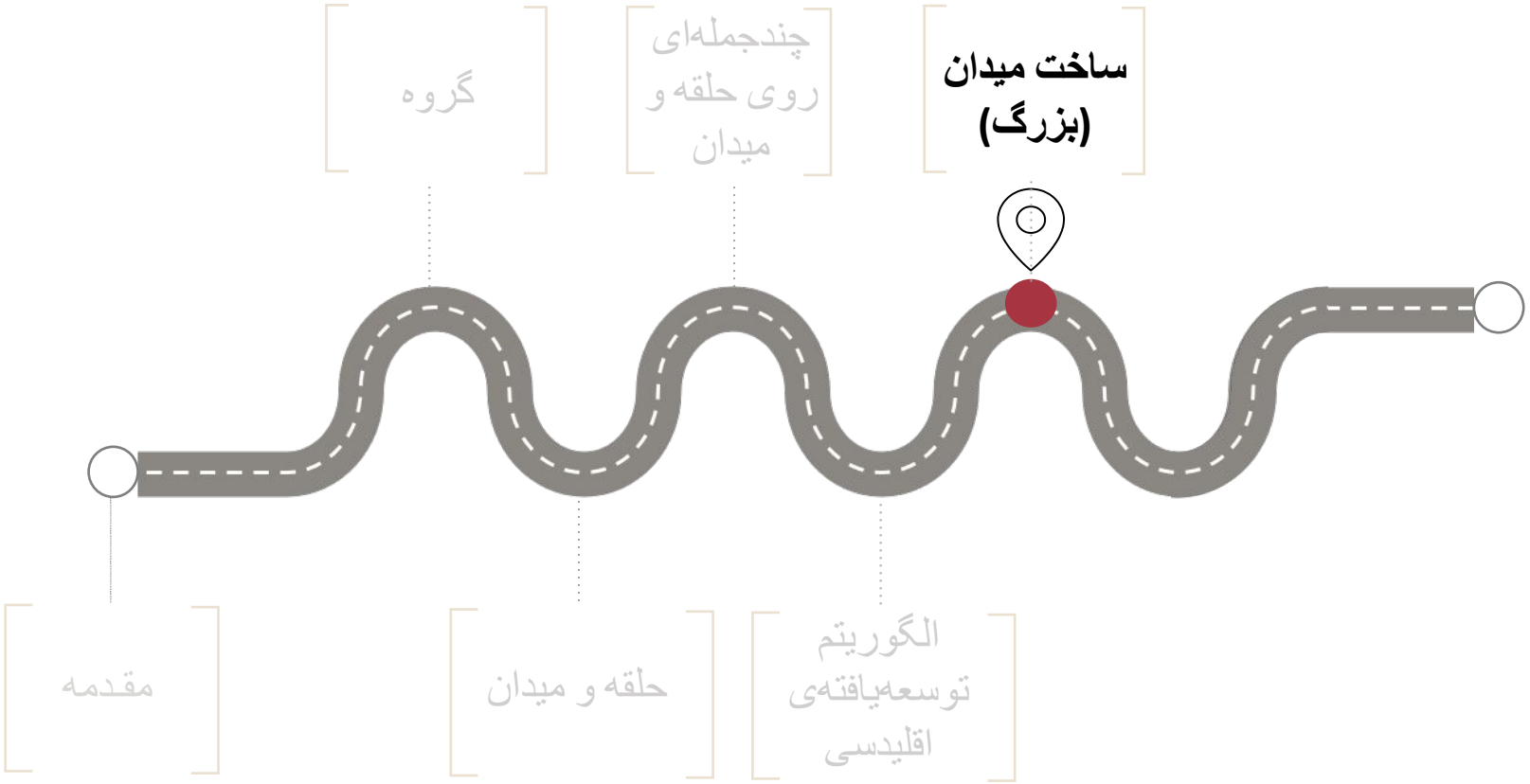
$$x^2(x^3+x^2+1)+(x^4+x+1)(x+1)=1$$
$$\Rightarrow x^2(x^3+x^2+1)\equiv 1 \mod (x^4+x+1)$$
$$\Rightarrow (x^2)^{-1}\equiv x^3+x^2+1 \mod (x^4+x+1)$$

- صحت رابطه‌ی فوق را می‌توان به‌سادگی بررسی کرد:

$$x^2(x^3+x^2+1)\equiv x^5+x^4+x^2 \mod (x^4+x+1)$$
$$\equiv (x^2+x)+(x+1)+x^2 \mod (x^4+x+1)$$
$$\equiv 2x^2+2x+1\equiv 1 \mod (x^4+x+1)$$

- در اثبات بالا از روابط زیر استفاده کرده‌ایم:

$$x^4+x+1\equiv 0 \mod (x^4+x+1)\Rightarrow x^4\equiv x+1$$
$$\Rightarrow x^5\equiv x^2+x$$


ساخت میدان
(بزرگ)
چندجمله‌ای
روی حلقه و
میدان
گروه
الگوریتم
توسعه‌یافته‌ی
اقلیدسی
حلقه و میدان
مقدمه

چندجمله‌ای تحویل‌ناپذیر

(Irreducible Polynomial)

- اگر F یک میدان و $f \in F[x]$ باشد، در این صورت f را روی $F[x]$ یک چندجمله‌ای تحویل‌ناپذیر گوییم، هرگاه:

1. $\deg(f) \geq 1$
2. $\text{if } f = gh \text{ , and } g, h \in F[x] \Rightarrow \deg(g) = 0 \quad \text{or} \quad \deg(h) = 0$

چندجمله‌ای اولیه

(Primitive Polynomial)

- **تعریف**: اگر $f(x) \neq 0$ یک چندجمله‌ای در $GF(2)$ باشد، در این صورت نما (یا Exponent) $f(x)$، کوچک‌ترین عدد صحیح e است که به ازای آن داشته باشیم: $f(x)|x^e + 1$.
- **لم**: اگر $f(x) \neq 0$ یک چندجمله‌ای درجه‌ی n در $GF(2)$ باشد، حداکثر مقدار نما برابر با $2^n - 1$ است.
- **تعریف**: اگر $f(x) \neq 0$ یک چندجمله‌ای درجه‌ی n در $GF(2)$ باشد، در این صورت آن را چندجمله‌ای اولیه گوییم هرگاه:
  1. $f(x)$ تحویل‌ناپذیر باشد.
  2. نمای آن ماکزیمم (یعنی $e = 2^n - 1$) باشد.

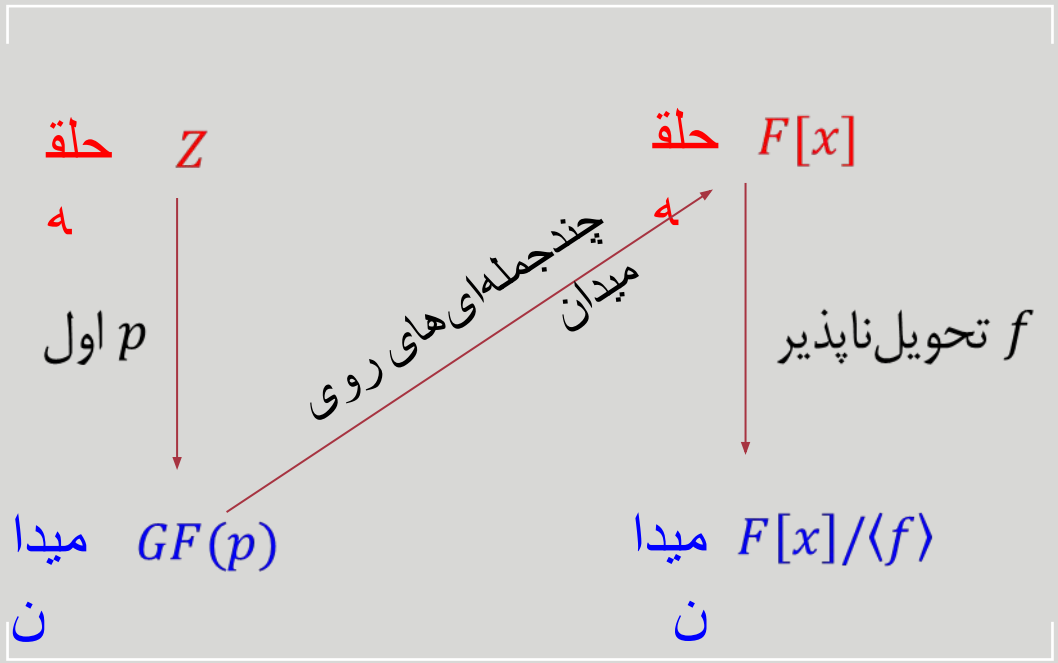
ساخت میدان با استفاده از $F[x]$

- **یادآوری:** $F[x]$ همراه با اعمال $+$ و $\times$، یک حلقه است (نه میدان) چراکه در حالت کلی همه‌ی اعضای $F(x)$ وارون ندارند.
- **قضیه:** اگر f یک چندجمله‌ای تحویل‌ناپذیر روی میدان F باشد، در این صورت $F[x]/\langle f\rangle$ همراه با اعمال $+$ و $\times$ تعریف‌شده روی میدان F، یک میدان تشکیل می‌دهد.
- منظور از $F[x]/\langle f\rangle$، چندجمله‌ای‌هایی با ضرائب عضو F هستند که در پیمانه‌ی f محاسبه شده باشند.
- بنابراین اگر f از درجه‌ی n باشد، $F[x]/\langle f\rangle$ شامل چندجمله‌ای‌های با درجه کم‌تر از n است که ضرائب آن‌ها عضو F هستند.

داریم چی می‌گیم؟! 😊

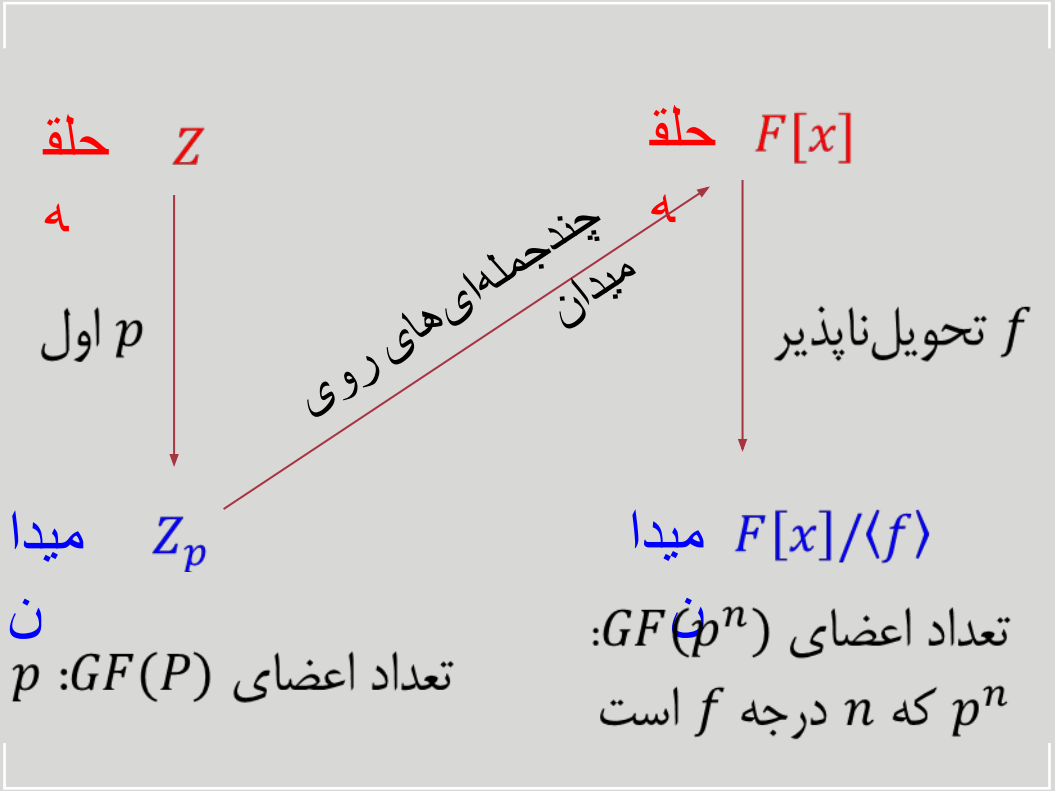
- آنچه تاکنون دیدیم:

- اگر حلقه نیاز داریم، Z حلقه است.
- اگر میدان نیاز داریم، Z_p میدان است.
- به دنبال ساخت میدان هستیم یا حلقه؟!



ساخت میدان‌های بزرگ

- میدان، زیرمجموعه‌ی حلقه است.
- محاسبات در میدان راحت‌تر است.
- هرچند در برخی کاربردها از میدان $GF(p)$ استفاده می‌شود اما $GF(p^n)$ نیز کاربرد دارد.
- چرا فقط از $GF(p)$ استفاده نکنیم؟
- $GF(p^n)$ تعداد اعضای بیشتری نسبت به $GF(p)$ دارد درحالی‌که محاسبات مربوط به ضرائب در پیمانه p است (تسهیل محاسبات).
- به خصوص استفاده از میدان $GF(2^n)$ متداول است چراکه منجر به تسهیل محاسبات می‌شود.

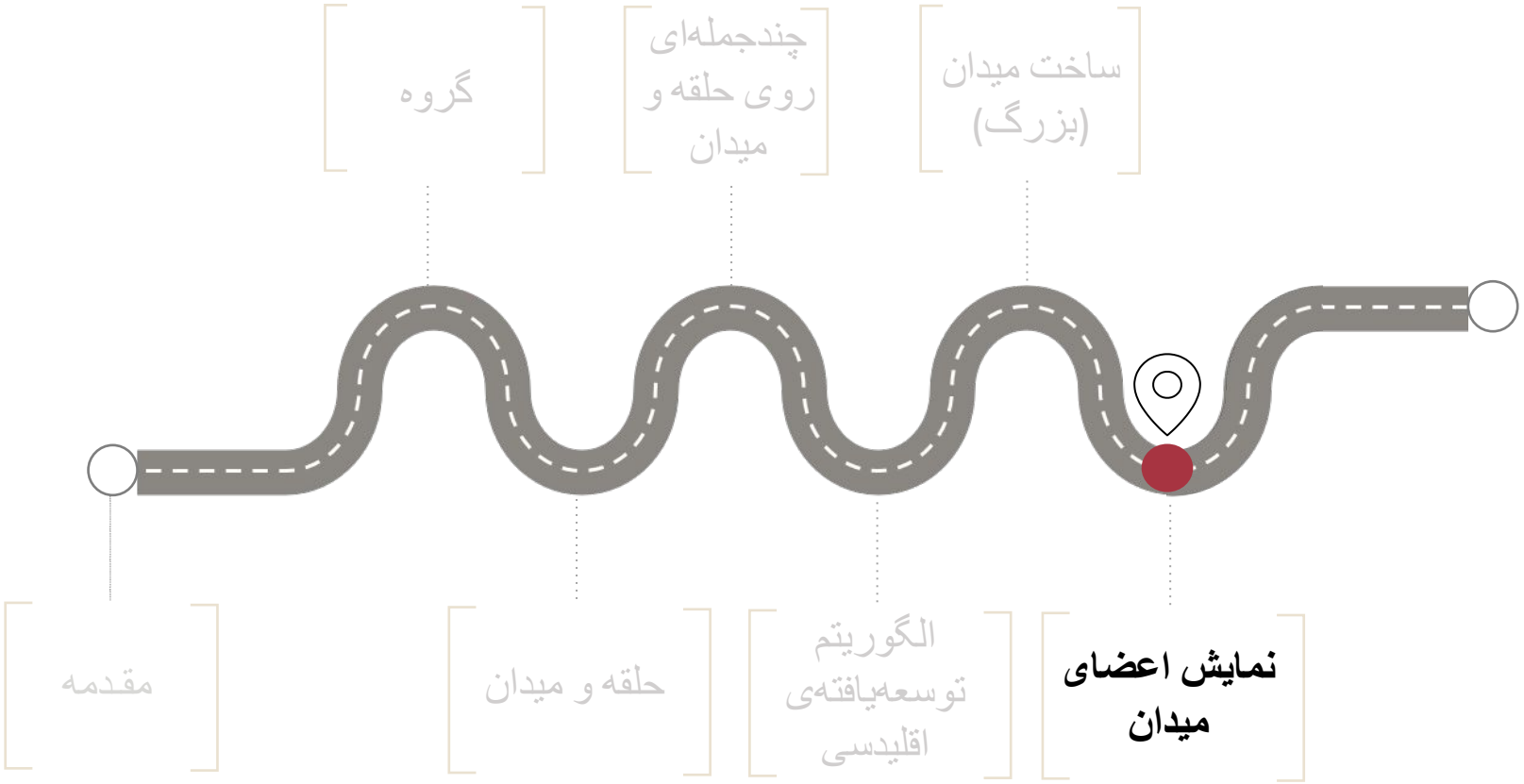


تسهیل محاسبات

- محاسبه‌ی $15 + 23$ در دو میدان مختلف $GF(2^5)$ و $GF(31)$:

$GF(2^5)$
01111
10111
11000
محاسبه به صورت موازی
امکان‌پذیر است (بدون کری بیت)
⇐
محاسبات با زمان و حافظه
کمتر امکان‌پذیر خواهند بود.

$GF(31)$
01111
10111
100110
00110
محاسبه به صورت
موازی امکان‌پذیر نیست
(کری بیت داریم)


ساخت میدان (بزرگ)
چندجمله‌ای روی حلقه و میدان
گروه
نمایش اعضای میدان
الگوریتم توسعه‌یافته‌ی اقلیدسی
حلقه و میدان
مقدمه

نمایش توانی اعضای میدان

- میدان $GF(p^n): GF(p)/\langle f \rangle$ را در نظر بگیرید که در آن f یک چندجمله‌ای تحویل‌ناپذیر از درجه n است.
- **قضیه:** اگر α ریشه‌ی چندجمله‌ای f باشد (یعنی $f(\alpha) = 0$)، مجموعه‌ی زیر شامل تمامی عناصر میدان است:

$$\{\alpha, \alpha^2, \dots, \alpha^{p^n-2}, \alpha^{p^n-1} = \alpha^0 = 1,0\}$$

- مرتبه‌ی α در میدان متناهی $GF(p^n)$ برابر $p^n - 1$ است، یعنی $\alpha^{p^n-1} = 1$.
- به عبارت دیگر، می‌توان تمام اعضای غیر صفر میدان را با استفاده از α تولید کرد.

تبدیل نمایش توانی به نمایش‌های دیگر

- از آنجایی‌که α ریشه‌ی چندجمله‌ای f است، داریم:

$$f(\alpha) = \sum_{i=1}^{n} a_i \alpha^i = 0$$

- بنابراین می‌توان توان‌های α را به صورت ترکیب خطی از مقادیر $\{\alpha^{n-1}, \dots, \alpha, 1\}$ و به شکل یک چندجمله‌ای نمایش داد:

$$a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0$$

- به صورت مشابه می‌توان عناصر میدان را به صورت بردار نمایش داد:

$$(a_{n-1}, \dots, a_1, a_0)$$

- مثال: میدان $GF(2^3): GF(2)/\langle x^3 + x + 1 \rangle$

نمایش برداری	نمایش چندجمله‌ای	نمایش توانی
	0	0
	1	1

کاربرد نمایش‌های مختلف

- عمل ضرب با استفاده از نمایش توانی راحت‌تر قابل محاسبه است:

$$\alpha^i \times \alpha^j = \alpha^{i+j \bmod p^n-1}$$

(یادآوری: مرتبه‌ی α در میدان متناهی $GF(p^n)$ برابر $p^n - 1$ است، یعنی:

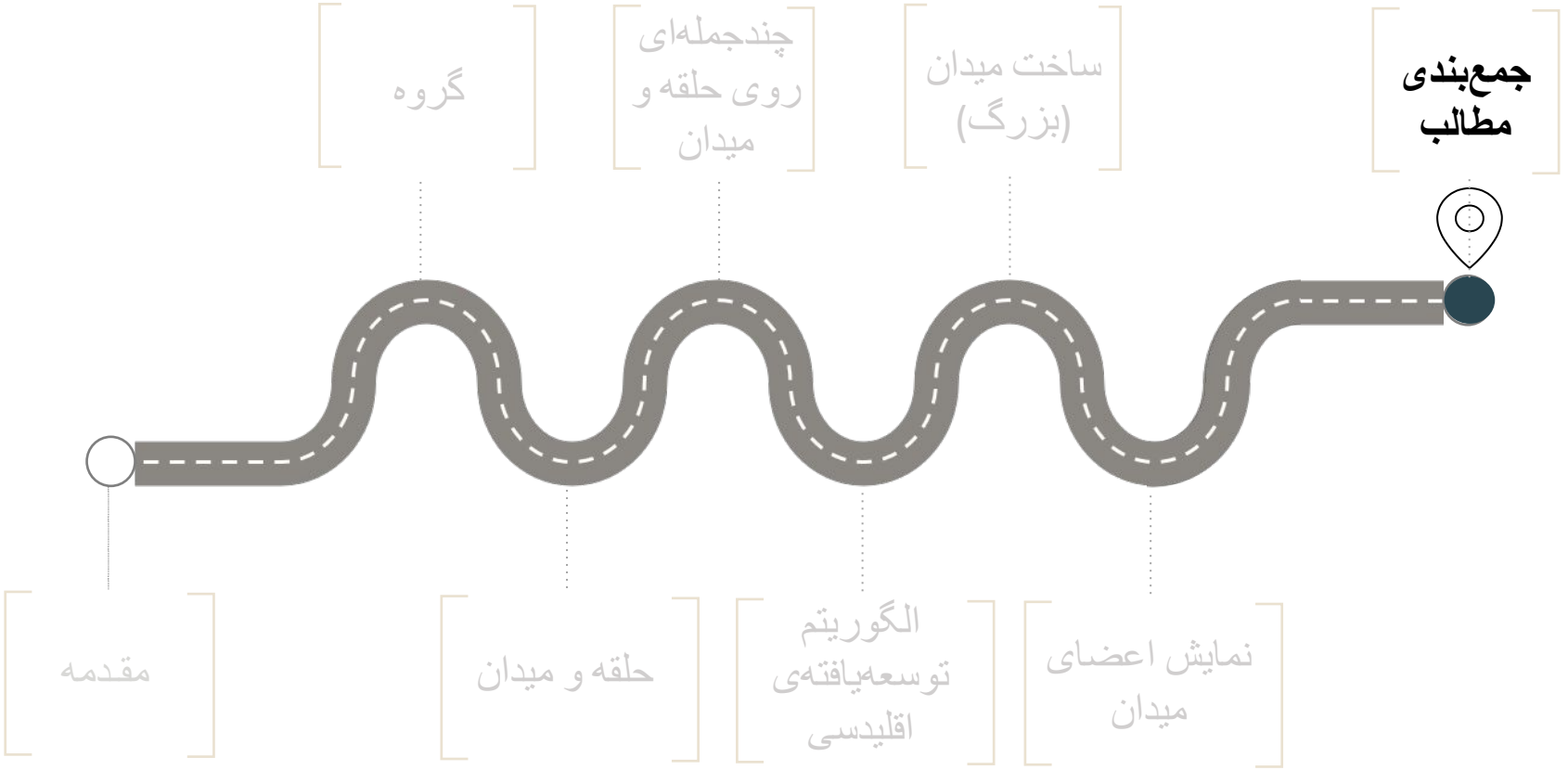
$$\alpha^{p^n-1} = 1 \ )$$

- مثال: برای میدان $GF(2^3): GF(2)[x]/\langle x^3 + x + 1\rangle$

$$\alpha^3 \times \alpha^4 = \alpha^{7 \bmod 7} = \alpha^0 = 1$$

- عمل جمع با استفاده از نمایش چندجمله‌ای راحت‌تر قابل محاسبه است.
- مثال: برای میدان فوق:

$$\alpha^3 + \alpha^4 = (\alpha + 1) + (\alpha^2 + \alpha) = \alpha^2 + 1$$


جمع‌بندی مطالب
ساخت میدان (بزرگ)
چندجمله‌ای روی حلقه و میدان
گروه
نمایش اعضای میدان
الگوریتم توسعه‌یافته‌ی اقلیدسی
حلقه و میدان
مقدمه

جمع‌بندی مطالب

- در این درس با مفاهیم اولیه‌ی گروه، حلقه و میدان آشنا شدیم.
- نحوه‌ی ساخت میدان‌های متناهی (بزرگ) را معرفی کردیم.
- دیدیم که برای نمایش اعضای میدان روش‌های مختلفی وجود دارد که براساس کاربرد مورد نیاز، از نمایش توانی یا چندجمله‌ای استفاده می‌شود.