نظریه گروه‌ها

- گروه (Group)
  - هر گروه G شامل مجموعه‌ای از عناصر همراه با یک عمل دوتایی $\circ$ است
    - عمل دوتایی $\circ$
      - جمع، ضرب و غیره
  - ویژگی‌ها
    - بستار (Closure)
      - برای هر $a,b \in G$
        - $a \circ b \in G$
    - شرکت‌پذیری (Associative)
      - برای هر $a,b,c \in G$
        - $a \circ (b \circ c) = (a \circ b) \circ c$

نظریه گروه‌ها

- عنصر همانی یا خنثی (Identity Element)
  - عنصری مانند $e \in G$ وجود دارد به طوری که برای هر $a \in G$
    - $a \circ e = e \circ a = a$
- عنصر وارون یا معکوس (Inverse Element)
  - برای هر $a \in G$ عنصری مانند $a^{-1} \in G$ وجود دارد به طوری که
    - $a \circ a^{-1} = a^{-1} \circ a = e$
- مثال
- مجموعه اعداد صحیح $Z_n = \{0,1,\dots,(n-1)\}$ و عمل جمع به پیمانه n یک گروه با عنصر همانی 0 است

نظریه گروه‌ها

- گروه آبلی (Abelian Group)
  - گروه $(G, \circ)$ آبلی نامیده می‌شود اگر برای هر $a, b \in G$
    - $a \circ b = b \circ a$
- با فرض این که Z_n^* مجموعه همه اعداد صحیح مثبتی باشد که از n کوچک‌تر بوده و نسبت به n اول هستند
  - Z_n^* یک گروه آبلی تحت عمل ضرب به پیمانه n است
    - عنصر همانی
      - $e = 1$
    - محاسبه معکوس ضربی
      - الگوریتم گسترش‌یافته اقلیدس یا قضیه اویلر

نظریه گروه‌ها

- **مثال**
  - Z_9^* **یک گروه آبلی تحت عمل ضرب به پیمانه 9 است**
    - $Z_9^* = \{1,2,4,5,7,8\}$
  - **جدول ضرب برای** Z_9^*

× mod 9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

نظریه گروه‌ها

- **گروه متناهی (Finite Group)**
  - گروه $(G, \circ)$ متناهی نامیده می‌شود اگر تعداد عناصرش متناهی باشد
  - کاردینالیتی یا مرتبه گروه
    - $|G|$
  - مثال
    - گروه متناهی $(Z_n, +)$
      - $|Z_n| = n$
    - گروه متناهی $(Z_n^*, \times)$
      - $|Z_n^*| = \varphi(n)$
    - گروه متناهی $(Z_9^*, \times)$
      - $|Z_9^*| = \varphi(9) = 3^2 - 3^1 = 6$

نظریه گروه‌ها

- مرتبه عناصر گروه
  - مرتبه هر عنصر $a \in G$ برابر با کوچک‌ترین عدد صحیح مثبت k است به طوری که $a^k = a \circ a \circ \cdots \circ a = e$
    - $ord(a) = k$
  - مثال
    - مرتبه عنصر 3 در گروه آبلی Z_{11}^*
      - $ord(3) = 5$

$$3^1 = 3 \equiv 3 \pmod{11}$$
$$3^2 = 9 \equiv 9 \pmod{11}$$
$$3^3 = 27 \equiv 5 \pmod{11}$$
$$3^4 = 81 \equiv 4 \pmod{11}$$
$$3^5 = 243 \equiv 1 \pmod{11}$$

نظریه گروه‌ها

- گروه دوری (Cyclic Group)
  - گروه $(G, \circ)$ دوری نامیده می‌شود اگر شامل حداقل یک عنصر g با حداکثر مرتبه $|G|$ باشد
    - $ord(g) = |G|$
      - عنصر g تمام گروه را تولید می‌کند
  - عناصر با حداکثر مرتبه
    - عناصر اولیه (Primitive Elements)
    - مولدها (Generators)
    - ریشه‌های اولیه (Primitive Roots)

نظریه گروه‌ها

- **مثال**
  - **گروه دوری Z_{11}^{*}**
    - **عنصر اولیه یا مولد**
      - **2**

$$2^1 \equiv 2 \pmod{11}$$
$$2^2 \equiv 4 \pmod{11}$$
$$2^3 \equiv 8 \pmod{11}$$
$$2^4 \equiv 5 \pmod{11}$$
$$2^5 \equiv 10 \pmod{11}$$
$$2^6 \equiv 9 \pmod{11}$$
$$2^7 \equiv 7 \pmod{11}$$
$$2^8 \equiv 3 \pmod{11}$$
$$2^9 \equiv 6 \pmod{11}$$
$$2^{10} \equiv 1 \pmod{11}$$

نظریه گروه‌ها

- برای هر عدد اول p گروه $(Z_p^*, \times)$ یک گروه دوری متناهی آبلی است
- با فرض این که $(G, \circ)$ یک گروه دوری متناهی باشد
  - مرتبه هر عنصر $a \in G$ یعنی $ord(a)$ مرتبه گروه یعنی $|G|$ را می‌شمارد
  - مثال
    - گروه دوری Z_{11}^*
    - $|Z_{11}^*| = 10$

$$
\begin{array}{lll}
ord(1) = 1 & ord(5) = 5 & ord(9) = 5 \\
ord(2) = 10 & ord(6) = 10 & ord(10) = 2 \\
ord(3) = 5 & ord(7) = 10 & \\
ord(4) = 5 & ord(8) = 10 &
\end{array}
$$

نظریه گروه‌ها

- با فرض این که $(G, \circ)$ یک گروه دوری متناهی باشد
  - تعداد عناصر اولیه G برابر با $\varphi(|G|)$ است
  - مثال
    - گروه دوری Z_{11}^{*}
      - $|Z_{11}^{*}| = 10$
      - $\varphi(10) = (5-1)(2-1) = 4$
      - عناصر اولیه
        - 2
        - 6
        - 7
        - 8

نظریه گروه‌ها

- زیرگروه (Subgroup)
  - زیرمجموعه‌ای از گروه $(G, \circ)$ که خودش تحت عمل $\circ$ یک گروه است
- با فرض این که $(G, \circ)$ یک گروه دوری متناهی باشد
  - هر عنصر $a \in G$ با مرتبه s یک عنصر اولیه از یک زیرگروه دوری با s عنصر است
  - مثال
    - گروه دوری Z_{11}^{*}
      - $ord(3) = 5$
    - زیرگروه دوری $H = \{1,3,4,5,9\}$
      - عنصر اولیه
        - 3

× mod 11	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

نظریه گروه‌ها

- **قضیه لاگرانژ**
  - **با فرض این که $(G, \circ)$ یک گروه دوری متناهی باشد**
    - **مرتبه هر زیرگروه $H \subseteq G$ یعنی $|H|$ مرتبه گروه یعنی $|G|$ را می‌شمارد**
  - **مثال**
    - **گروه دوری Z_{11}^***
      - $|Z_{11}^*| = 10 = 1 \times 2 \times 5$
    - **زیرگروه‌های دوری**
      - $H_1 = \{1\}$
      - $H_2 = \{1,10\}$
      - $H_3 = \{1,3,4,5,9\}$

نظریه گروه‌ها

- با فرض این که $(G, \circ)$ یک گروه دوری متناهی و g یک عنصر اولیه برای این گروه باشد
  - برای هر عدد صحیح k که مرتبه گروه یعنی $|G|$ را می‌شمارد تنها یک زیرگروه دوری $H \subseteq G$ از مرتبه k وجود دارد
    - زیرگروه دوری H توسط $g^{|G|/k}$ تولید می‌شود
  - مثال
    - گروه دوری Z_{11}^*
      - عنصر اولیه
        - 8
    - عنصر اولیه یا مولد برای زیرگروه دوری از مرتبه 2
      - $8^{10/2} = 8^5 \equiv 10 \pmod{11}$

نظریه گروه‌ها

- **تمرین**
  - **ثابت کنید عدد صحیح x یک عنصر اولیه برای گروه دوری Z_{97}^{*} است اگر و فقط اگر $x^{32} \not\equiv 1 \pmod{97}$ و $x^{48} \not\equiv 1 \pmod{97}$**

مساله لگاریتم گسسته

- با فرض این که p یک عدد اول، Z_p^* یک گروه دوری متناهی و $g \in Z_p^*$ یک عنصر اولیه برای این گروه باشد
  - هدف مساله لگاریتم گسسته یافتن عدد صحیح $1 \leq x \leq p-1$ است به طوری که $g^x \equiv \beta \pmod{p}$
    - عدد صحیح x
      - لگاریتم گسسته β به مبنای g

$$x = \log_g \beta \mod p$$

  - مثال
    - گروه دوری Z_{47}^*
      - مساله لگاریتم گسسته
        - یافتن عدد صحیح مثبت $1 \leq x \leq 46$ به طوری که $5^x \equiv 41 \pmod{47}$

مساله لگاریتم گسسته

- محاسبه لگاریتم‌های گسسته به پیمانه یک عدد اول یک مساله سخت است
- در صورتی که مرتبه گروه اول باشد، از حمله پولیگ-هلمن جلوگیری می‌شود
  - مرتبه گروه دوری Z_p^* اول نیست
    - $|Z_p^*| = p - 1$
  - برای جلوگیری از حمله پولیگ-هلمن، اغلب مساله لگاریتم گسسته به جای Z_p^* در زیرگروه‌هایی از Z_p^* با مرتبه اول استفاده می‌شود

مساله لگاریتم گسسته

- مثال
  - گروه دوری Z_{47}^{*}
    - $|Z_{47}^{*}| = 46$
  - مرتبه زیرگروه‌های Z_{47}^{*} با توجه به قضیه لاگرانژ
    - $|H_1| = 1$
    - $|H_2| = 2$
    - $|H_3| = 23$
  - عنصر اولیه یا مولد برای زیرگروه دوری H_3
    - $g = 2$
  - با فرض این که $\beta = 36$
    - مساله لگاریتم گسسته
      - یافتن عدد صحیح مثبت $1 \le x \le 23$ به طوری که $2^x \equiv 36 \pmod{47}$