گروه ضربی اعداد به پیمانه n (Z_n^*)

پارسا تسبیح‌گو، صالح مستانی، محمدرضا معتبر

۲۸ تیر ۱۴۰۱

چکیده

در این متن به بررسی ساختار و خواص گروه Z_n^* به ویژه در حالتی که این گروه دوری است می‌پردازیم. در ادامه مسائل مربوط و کاربردهایی از گروه Z_n^* را مطرح می‌کنیم و تاثیر این گروه در رمزنگاری را تحلیل می‌کنیم.

۱ مقدمه

تعریف ۱. اگر n عدد طبیعی باشد آنگاه گروه Z_n^* را چنین تعریف می‌کنیم:

$$Z_n^* = \{a \in Z_n^+ |\ \gcd(a, n) = ۱\}$$

اکنون ثابت می‌کنیم Z_n^* در اصول موضوعه صادق است.

۱. Z_n^* دارای عضو خنثی است.

برهان. می‌دانیم $\gcd(۱, n) = ۱$ ، لذا $۱ \in Z_n^*$ و طبق تعریف ضرب روی اعداد طبیعی ۱ همواره عضو خنثی می‌باشد.

۲. Z_n^* نسبت به عمل معرفی شده (از حالا با $\cdot$ نمایش می‌دهیم) بسته است.

برهان. دو عضو دلخواه a و b در Z_n^* را در نظر بگیرید اگر $a \cdot b \notin Z_n^*$ ، پس $\gcd(a \cdot b, n) = d > ۱$ ، در نتیجه عدد اول p چنان وجود دارد که $p|d$ ، مطابق تعریف gcd می‌توان گفت $p|a$ یا $p|b$ بدون از دست دادن کلیات مسئله فرض کنیم $p|a$ ، همچنین می‌دانیم چون $d|n$ پس $p|n$ در نتیجه $\gcd(a, n) \geq p$ که با فرض $a \in Z_n^*$ متناقض است. در نتیجه فرض خلف باطل و $a \cdot b \in Z_n^*$.

۳. عمل . شرکت پذیر است.

برهان. از تعریف ضرب روی اعداد طبیعی نتیجه می‌شود ، ۰ شرکت پذیر است.

۴. هر عضو در Z_n^* دارای وارون می‌باشد.

برهان. عضو a را به طور دلخواه از Z_n^* انتخاب می‌کنیم، می‌توان گفت $\gcd(a,n) = ۱$.
حال طبق لم بزو اعداد x و y چنان موجود هستند که $ax + ny = ۱$ این معادله به پیمانه n نیز باید برقرار باشد، در نتیجه $ax + ny \overset{n}{\equiv} ۱$ پس $ax \overset{n}{\equiv} ۱$ همچنین ادعا می‌کنیم x نسبت به n اول است زیرا:
فرض کنیم $\gcd(x,n) = d$ ، آنگاه چون $ax + ny = ۱$ می‌توان گفت $d(ax' + n'y) = ۱$ پس $dA = ۱$ از آنجا که A عددی صحیح است پس ۱ مضربی صحیح از d است، لذا تنها حالت ممکن برای d ، برابر بودنش با ۱ است.
در نتیجه $\gcd(x,n) = ۱$ پس $x \in Z_n^*$ و $ax \overset{n}{\equiv} ۱$.

نشان دادیم Z_n^* در اصول موضوعه گروه صادق است ، در نتیجه Z_n^* گروه است.

لم ۱ (بزو)**.** فرض کنیم $n, m \in \mathbb{N}$ آنگاه $a, b \in \mathbb{Z}$ چنان موجود هستند که $an + bm = \gcd(n,m)$.

برهان. تعریف می‌کنیم $S = \{an + bm \mid a, b \in \mathbb{Z} \wedge an + bm > ۰\}$.
طبق اصل خوش ترتیبی می‌دانیم S دارای کوچکترین عضو می‌باشد ، آن را d می‌نامیم، (S ناتهی است زیرا دست کم a یا $-a$ عضو S است)،

۱. ثابت می‌کنیم $d|n$ و $d|m$.
طبق الگوریتم تقسیم می‌دانیم $n = dq + r (۰ \leq r < d)$ همچنین داریم:

$$r = n - dq = n - (an + bm)q = n(۱ - aq) + m(bq)$$

پس یا $r = ۰$ یا $r \in S$ اگر $r \in S$ پس $d \leq r$ که تناقض است در نتیجه $d|n$. برهان مشابه ثابت می‌کند $d|m$.

۲. ثابت می‌کنیم هر مقسوم علیه مشترک n و m مثل t ، کمتر مساوی d است.
فرض کنیم $n = tu$ و $m = tv$ در نتیجه

$$d = tua + tvb = t(ua + vb)$$

پس $t|d$ پس $t \leq d$.

به این ترتیب حکم ثابت می‌شود.

۲ قضایا

قضیه ۱. Z_n^* گروه آبلی است.

اثبات ۱. طبق تعریف ضرب روی اعداد طبیعی ، ضرب جابه‌جایی می‌باشد، در نتیجه $\cdot$ نیز جابه‌جایی است.

مثال. جدول ضرب $Z_۸^*$:

۷	۵	۳	۱	$\cdot$
۷	۵	۳	۱	۱
۵	۷	۱	۳	۳
۳	۱	۷	۵	۵
۱	۳	۵	۷	۷

حال تعداد اعضای گروه Z_n^* را بررسی می‌کنیم.

تعریف ۲. تابع اویلر را با $\varphi(n)$ نمایش می‌دهیم و به این شکل تعریف می‌کنیم:

$$\varphi : \mathbb{N} \to \mathbb{N}$$

$$\varphi(n) = |Z_n^*|$$

این تابع را تابع اویلر گویند از آن جهت که نخستین بار اویلر در سال ۱۷۶۳ میلادی آن را معرفی کرد و آن را با π نمایش می‌دهند.
اما صورت امروزی آن توسط گاوس در سال ۱۸۰۱ میلادی معرفی شد.
لازم به ذکر است تابع φ نخستین بار برای بیان تعداد اعداد طبیعی کوچکتر از n که نسبت به آن اول هستند معرفی شد.

قضیه ۲. اویلر برای محاسبه $\varphi(n)$ فرمول زیر را ارائه کرد:

$$\varphi(n) = n \prod_{p|n} (۱ - \frac{۱}{p})$$

اثبات ۲. فرض کنیم $n = \prod_{i=۱}^{r} p_i^{\alpha_i}$، به ازای هر $۱ \leq i \leq r$ ، قرار دهیم $A_i = \{k \in \mathbb{N} \mid p_i | k \wedge k \leq n\}$ طبق اصل شمول و عدم شمول داریم:

$$\varphi(n) = n - |\cup_{i=۱}^{r} A_i|$$

از آنجایی که اعضای A_i مضارب p_i هستند، $|A_i| = \frac{n}{p_i}$ ، همچنین به ازای هر $i \neq j$ اعضای $|A_i \cap A_j|$ مضارب p_i و p_j هستند لذا $|A_i \cap A_j| = \frac{n}{p_i p_j}$ ، به همین ترتیب برای هر $i_۱ < \cdots < i_t$ داریم $|\cap_{k=۱}^{m} A_{i_k}| = \frac{n}{\prod_{k=۱}^{m} p_{i_k}}$ پس:

$$\varphi(n) = n(۱ - \frac{۱}{p_۱}) \cdots (۱ - \frac{۱}{p_r})$$

نتیجه. ۱. $\varphi(n \times m) = \varphi(n) \times \varphi(m) \times \frac{\gcd(n,m)}{\varphi(\gcd(n,m))}$.

۲. $\varphi(p^k) = p^{k-1}(p-1)$.

در قضیه ۱ نشان دادیم Z_n^* آبلی است، اما برای شناخت بهتر Z_n^* باید بدانیم آیا Z_n^* دوری است؟
پیش از بررسی دوری بودن Z_n^* خوب است به مفهومی معادل در نظریه اعداد بپردازیم.

تعریف ۳. اگر n عددی طبیعی فرض کنیم اعداد $\{0, 1, 2, \cdots, n-1\}$ توسط رابطه R_n که به این شکل تعریف میشود:

$$a \; R_n \; b \iff a \overset{n}{\equiv} b$$

به تعدادی کلاس هم ارزی افراز می‌شود.

تعریف ۴. اگر n را عددی طبیعی فرض کنیم g را یک ریشه اولیه برای n گوییم هرگاه $[g]_{R_n} \neq [0]_{R_n}$ و برای هر $x \in \mathbb{N}$ که $x < n$ و $[x]_{R_n} \neq [0]_{R_n}$ عدد طبیعی k چنان موجود باشد که $x = gk$.
این مفهوم توسط اویلر معرفی شد و گاوس در کتاب ۱۸۰۱ به طور گسترده به آن پرداخته است.

تعریف ۵. می‌دانیم همه گروه‌های دوری مرتبه n یکریخت هستند.
گروه دوری مرتبه n را در حالت کلی با C_n نمایش میدهیم و عمل آن $*$ است.

تعریف ۶. گروه چهارتایی کلاین را با K_4 نمایش می‌دهیم.

قضیه ۳. برای هر عدد n طبیعی C_n به ازای هر $d < n$ که $d|n$ دقیقا یک زیر گروه d عضوی دارد، همچنین زیرگروه دیگری ندارد.

اثبات ۳. طبق قضیه لاگرانژ اگر $H \leq C_n$ آنگاه $|H||n$. پس اگر C_n زیرگروه d عضوی داشته باشد $d|n$.
حال ثابت می‌کنیم برای هر $d < n$ که $d|n$ دقیقا یک زیرگروه d عضوی داریم.
می‌دانیم اگر $C_n = \langle g \rangle$ آنگاه $|\langle g^{\frac{n}{d}} \rangle| = d$ و $\langle g^{\frac{n}{d}} \rangle \leq C_n$.
حال ثابت می‌کنیم $\langle g^{\frac{n}{d}} \rangle$ تنها زیرگروه d عضوی است.
فرض کنیم $\langle g^\alpha \rangle$ زیر گروهی d عضوی باشد. طبق الگوریتم تقسیم می‌توان گفت $\alpha = \frac{n}{d}q + r \quad (r < \frac{n}{d})$ ، در نتیجه $rd < n$.

$$(g^\alpha)^d = (g^{\frac{n}{d}q+r})^d = g^{qn} * g^{rd} = e$$

چون $g^{qn} = e$ پس:

$$e * g^{rd} = e$$

چون $rd < n$ پس:

$$rd = 0$$

چون $d \neq 0$ پس:

$$r = 0$$

درنتیجه $g^{\alpha} = g^{\frac{n}{d}q}$ و $g^{\alpha} \in \langle g^{\frac{n}{d}} \rangle$
نهایتا:

$$\langle g^{\alpha} \rangle = \langle g^{\frac{n}{d}} \rangle$$

قضیه ۴. اگر فرض کنیم G یک گروه متناهی باشد ، $H \leq G$ موجود باشد طوری که $H \cong K_4$ ،آنگاه G دوری نیست.

اثبات ۴. فرض کنیم $G \cong C_n$ ،طبق قضیه ۳ ، G تنها یک زیر گروه مرتبه ۲ ممکن است داشته باشد، اما از آنجایی که $H = \{e, a, b, c\} \leq G$ و $H \cong K_4$ در نتیجه $a^2 = b^2 = c^2 = e$ پس G دست کم ۳ زیرگروه $\langle a \rangle$ و $\langle b \rangle$ و $\langle c \rangle$ را از مرتبه ۲ دارد، لذا فرض خلف باطل است و G دوری نیست.

تعریف ۷. اگر G را گروه فرض کنیم، تابع ψ_G را چنین تعریف می‌کنیم:

$$\psi_G : \mathbb{N} \to \mathbb{N}$$

$$\psi_G(m) = |\{x \in G | ord(x) = m\}|$$

قضیه ۵. $\sum_{d|n} \psi_G(d) = n$.

اثبات ۵. C_n را در نظر بگیریم ، هر عضو C_n مرتبه مشخصی دارد که طبق قضیه لاگرانژ n را می‌شمارد.
در نتیجه در حاصل جمع فوق هر عضو دقیقا یکبار شمارش شده و تعداد اعضا n است پس حاصل جمع فوق برابر n است.

قضیه ۶. C_n دقیقا $\varphi(n)$ سازنده دارد.

اثبات ۶. ابتدا ثابت می‌کنیم تعداد سازنده‌های C_n کمتر یا مساوی $\varphi(n)$ است.
فرض کنیم $C_n = \langle g \rangle$ ،اگر $g^k (k < n)$ نیز یک سازنده برای C_n باشد در نتیجه $ord(g^k) = n$ همچنین فرض کنیم $\gcd(k, n) = d$ ، حال می‌توان گفت:

$$(g^k)^{\frac{n}{d}} = (g^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$$

پس $ord(g^k) \leq \frac{n}{d}$ در نتیجه $n \leq \frac{n}{d}$ پس $d = 1$.
پس توان هر سازنده C_n نسبت به n اول است.
حال ثابت می‌کنیم اگر $\gcd(k, n) = 1$ آنگاه $ord(g^k) = n$.
فرض کنیم $ord(g^k) = m$ ، در نتیجه $g^{km} = e$ ، پس $n|km$ از آنجا که $\gcd(k, n) = 1$ پس $n|m$ پس $n \leq m$
از طرفی مرتبه هر عضو در گروه کمتر یا مساوی مرتبه گروه است یعنی $m \leq n$ در نتیجه $ord(g^k) = m = n$ پس $C_n = \langle g^k \rangle$.
به این ترتیب حکم ثابت شد.

قضیه ۷. $\sum_{d|n} \varphi(d) = n$.

اثبات ۷. C_n را در نظر بگیریم، هر عضو آن مثل x زیر گروهی مثل $\langle x \rangle$ تولید می‌کند که یکتاست.
طبق قضیه لاگرانژ (یا قضیه ۳) می‌دانیم $t = |\langle x \rangle| \mid n$ ، همچنین برای هر عضو بجز x که $|\langle y \rangle| = t$ ، طبق قضیه ۳ $\langle y \rangle = \langle x \rangle$ ، از این به بعد زیر گروه t عضوی C_n را H_t می‌نامیم و می‌دانیم H_t یکتا است، طبق قضیه ۶ H_t ، $\varphi(t)$ سازنده دارد، از آنجا کا با ازای هر $x \in C_n$ ، $ord(x)|n$ و برای هر $d < n$ که $d|n$ ، H_d ، $\varphi(d)$ سازنده دارد پس هر عضو در حاصل جمع بالا دقیقا یک بار شمارش شده و همچنین n عضو موجود است، لذا $\sum_{d|n} \varphi(d) = n$.

نتیجه. از قضیه ۵ و ۷ نتیجه می‌گیریم:

$$\sum_{d|n} \psi(d) = \sum_{d|n} \varphi(d)$$

قضیه ۸. اگر $k \in \mathbb{N}$ و $k > ۲$ و $n = ۲^k$ آنگاه Z_n^* دوری نیست.

اثبات ۸. گروه G را چنین تعریف می‌کنیم $G = \{۱, -۱, ۲^{k-۱} - ۱, ۲^{k-۱} + ۱\}$ توجه کنید که -۱ به پیمانه n همان $۲^k - ۱$ است. روشن است که $G \leq Z_n^*$ ، حالا نشان می‌دهیم $G \cong K_۴$.

$$(۲^k - ۱)^۲ \equiv ۲^{۲k} - ۲ \times ۲^k + ۱ \equiv ۰ - ۰ + ۱ \equiv ۱ \mod n$$
$$(۲^{k-۱} - ۱)^۲ \equiv ۲^{۲k-۲} - ۲^k + ۱ \equiv ۲^k \times ۲^{k-۲} - ۲^k + ۱ \equiv ۰ - ۰ + ۱ \equiv ۱ \mod n$$
$$(۲^{k-۱} + ۱)^۲ \equiv ۲^{۲k-۲} + ۲^k + ۱ \equiv ۲^k \times ۲^{k-۲} + ۲^k + ۱ \equiv ۰ - ۰ + ۱ \equiv ۱ \mod n$$

حال طبق قضیه ۴ می‌توان نتیجه گرفت Z_n^* دوری نیست.

قضیه ۹. در Z_p^* به ازای هر d داریم $\psi(d) = ۰$ یا $\psi(d) = \varphi(d)$.

اثبات ۹. اگر هیچ $a \in Z_p^*$ موجود نباشد که $ord(a) = d$ پس $\psi(d) = ۰$.
حال فرض می‌کنیم $a \in Z_p^*$ و $ord(a) = d$. از آنجا که معادله $\Gamma : x^d \equiv ۱ \mod p$ حداکثر d جواب دارد و همه اعضا دنباله $D : a, a^۲, \cdots, a^d$ متفاوت هستند و $(a^i)^d \overset{p}{\equiv} ۱$ (خاصیت زیرگروه دوری) لذا تمامی جواب‌های معادله Γ در میان دنباله D هستند، در نتیجه هر عضو $b \in Z_p^*$ که $ord(b) = d$ ، می‌توان نتیجه گرفت $b \in D$.
از تعریف دنباله D روشن است که اعضا D همان اعضا $\langle a \rangle$ هستند و لذا $|\langle a \rangle| = d$ همچنین هر عضو مثل $b \in Z_p^*$ که $ord(b) = d$ یک سازنده برای $\langle a \rangle$ است، با توجه به قضیه ۶ می‌توان گفت $\langle a \rangle$ ، $\varphi(d)$ سازنده دارد در نتیجه در کل $\varphi(d)$ عضو از Z_p^* از مرتبه d موجود است ، پس $\psi(d) = \varphi(d)$.

نتیجه. از نتیجه قضیه ۷ و قضیه ۹ می‌توان نتیجه گرفت در Z_p^* به ازای هر d که $d \big| |Z_p^*|$ ، $\psi(d) = \varphi(d)$ پس $\psi(|Z_p^*|) \neq ۰$ لذا Z_p^* دارای عضوی مثل g از مرتبه $|Z_p^*|$ است پس $Z_p^* =< g >$ در نتیجه Z_p^* دوری است.

مراجع

[1] Gauss, Carl Friedrich. *Disquisitiones arithmeticae*. Translated by Arthur A. Clarke. Springer, 1986

[2] Shoup, Victor. *A computational introduction to number theory and algebra*. Cambridge university press, 2009.

[3] Witno, Amin. The primitive root theorem. (`www.witno.com/numbers/chap5.pdf`)

شکل ۱: Carl Friedrich Gauss