SzA XIV. gyakorlat

Absztrakt algebrát akarunk alkalmazni, továbbá egyebek, meg a félévnek is vége

2012. december 6.

Feladatok

1. **Csoportot alkotnak-e az alábbi H halmazok a megadott műveletekre?**

   (a) $H = \{2k : k \in \mathbb{Z}\}$**, a művelet pedig az összeadás.**
   A műveletség rendben van, hiszen páros egész számokat összeadva páros egész számokat kapunk. Az asszociativitás is OK, az összeadás tudjuk, hogy asszociatív. Az egységelem a 0, hiszen $0 + 2k = 2k$. Inverz is van, $2k + (-2k) = 0$. Tehát csoport, ráadásul az összeadás kommutativitása miatt még Abel-csoport is.

   (b) $H = \mathbb{Z}$ **az egész számok halmaza, a művelet pedig az osztás.**
   Az osztás nem művelet, hiszen két egész számot elosztva egymással nem biztos, hogy egész számot kapunk.

   (c) $H = \mathbb{R}$ **a valós számok halmaza, a művelet pedig a hatványozás.**
   0^0 nem értelmezett, így még csak nem is művelet. $H = \mathbb{R} \setminus \{0\}$ halmaz esetén még mindig nem lenne művelet, pl $(-1)^{\frac{1}{2}}$ nem lesz valós szám.

   (d) $H = \mathbb{Z}^+$ **a pozitív egész számok halmaza, a művelet pedig a hatványozás.**
   A műveletséggel már nincs probléma, hiszen pozitív egészet egy pozitív egész hatványra emelve pozitív egész számot kapunk. Az asszociativitással viszont probléma lesz, házi feladat egy példát hozni erre.

   (e) H **egy tetszőleges** X **halmaz összes részhalmazainak halmaza, a művelet a halmazok szimmetrikus differenciája. Az** A **és** B **halmazok szimmetrikus differenciája alatt az** $A \triangle B = (A \setminus B) \bigcup (B \setminus A)$ **halmazt értjük.**
   Műveletnek művelet, hiszen az eredmény mindig egy X-beli (esetleg üres) részhalmaz. Az asszociativitás is rendben van, házi feladat ennek ellenőrzése. Az egységelem $\emptyset$, hiszen $A \triangle \emptyset = A$. Inverz is van, mégpedig minden elemnek önmaga az inverze, hiszen $A \triangle A = \emptyset$. Vagyis csoportunk van. Ráadásul a művelet még kommutatív is, vagyis még Abel-csoport is.

2. **Mik a** D_3 **diédercsoport elemei? Mik az elemek rendjei? Ciklikus-e ez a csoport? Adjuk meg** D_3 **egy ciklikus részcsoportját!**
   A D_3 definíciója megtalálható a jegyzetben. A helybenhagyás rendje 1, a másik két forgatás rendje 3, a tükrözések rendjei 2. A csoport nem ciklikus, hiszen sem a forgatásokkal, sem a tükrözésekkel nem lehet generálni az egészet. Egy ciklikus részcsoport pl. az egységelem és egy tükrözés.

3. **Hány olyan eleme van a** C_{12} **ciklikus csoportnak, ami egymaga generálja az egész csoportot? És** C_n**-nek?**
   C_{12} eset: nyilván e nem generálja az egészet, g igen (nevezzük g-nek az elemet, amiből generáltuk; tudjuk, hogy a rendje 12). g^2 nem, mert $(g^2)^6 = g^{12} = e$, hasonló okokból g^3 sem, g^4 sem, stb. Egyrészt végiginézhetjük az összes elemet, másrészt rájöhetünk, hogy pontosan azon g^i-k generálják az egész csoportot, ahol $(i, 12) = 1$. És hogy ezekből hány darab van? Ez ugye az 1 és 12 közötti, 12-höz relatív prímek száma. Ami pont $\varphi(12) = 4$, feltéve, hogy jól számoltam. És általánosítva a válasz: $\varphi(n)$.

4. **Írjuk fel $\pi \circ \rho$-t, ha**

$$\begin{aligned} \pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 8 & 4 & 2 & 7 & 6 & 3 \end{pmatrix} \\ \rho &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 1 & 8 & 7 & 4 & 6 & 3 \end{pmatrix} \\ \pi \circ \rho &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 3 & 8 & 2 & 6 & 4 & 1 \end{pmatrix} \end{aligned}$$

Megjegyzés: ez nincs benne az idei anyagban. Persze nem tilos tudni :D

5. **Tekintsünk egy páratlan rendű Abel-csoportot, ahol a művelet neve az összeadás. Bizonyítsuk be, hogy az összes elem összege 0, azaz az egység! (Vagyis a csoport összes elemét összeadjuk.)**
Kezdjük el összegezni az elemeket! Mivel mindenkinek az inverze szerepel a csoportban (definíció szerint), valamint az inverz egyértelmű, bizonyos elemek az inverzükkel együtt szerepelnek az összegben, így ők páronként pont az egységelemet adják (a kommutativitás miatt tetszőleges az összeadás sorrendje). Ezen elemek pont azok, akik nem önmaguk inverzei. Így

$$\sum_{g \in G} g = \sum_{g \in G, g^{-1} \neq g} g + \sum_{g \in G, g^{-1} = g} g = 0 + \sum_{g \in G, g^{-1} = g} g = \sum_{g \in G, g^{-1} = g} g.$$

A maradék összegben biztos szerepel az egységelem, ami nem zavar minket. Tfh más is szerepel, azaz $\exists g \in G \neq 0 : g^2 = 0$. Ekkor az ő rendje 2, ami lehetetlen, hiszen az elem rendje osztja a csoport rendjét, vagyis 2 osztana egy ptlan számot. Tehát a maradék összegben kizárólag az egység szerepel, és pont ezt akartuk bizonyítani.

6. **Tudjuk, hogy a G csoport rendje 100, a g elemre pedig teljesül, hogy $g^{21} = e$. Mit tudunk g-ről?**
Tudjuk, hogy g rendje 1, 3, 7, vagy 21. De mivel a rendje osztja a csoport rendjét, ezért 3, 7, és 21 nem lehet, vagyis a rendje 1, azaz $g = e$.

7. **Melyik alkot gyűrűt, és melyik alkot testet?**

   (a) $\langle \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}, \{+, \cdot\} \rangle$
   Az összeadásra nézve Abel-csoport, hiszen zárt, asszociatív (kéretik ellenőrizni) egységelem a $0 + 0\sqrt{2}$, $a + b\sqrt{2}$ inverze $-a - b\sqrt{2}$. A szorzás nyilván félcsoport (zárt, asszociatív; ezt kéretik ellenőrizni), továbbá a disztributivitás is teljesül (kéretik ellenőrizni). Ha a 0-t kivesszük a halmazból, akkor a szorzásra nézve csoport, hiszen csak az egységet és inverzet kell ellenőrizni, amik rendre $1 + 0\sqrt{2}$ és $a + b\sqrt{2}$ esetén $\frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2}$ (nevező gyöktelenítéssel dolgozva jött ki). Tehát test.

   (b) $\langle \{a + b\sqrt[3]{2} : \ a, b \in \mathbb{Q}\}, \{+, \cdot\} \rangle$
   A szorzás nem lesz művelet, hiszen pl. $(0 + 1 \cdot \sqrt[3]{2})(0 + 1 \cdot \sqrt[3]{2}) = (\sqrt[3]{2})^2$, ami nem eleme a halmazunknak. Tehát még csak nem is gyűrű.

   (c) $\langle \{\frac{a}{b} : \ a, b \in \mathbb{Z}, 2 \nmid b, 5 \nmid b\}, \{+, \cdot\} \rangle$
   Az összeadás Abel-csoport (ellenőrizendő!), a szorzás Abel-félcsoport (ellenőrizendő!), a disztributivitás teljesül (ellenőrizendő!). A szorzásnak viszont nincs inverze, hiszen pl $\frac{5}{1}$ inverze $\frac{1}{5}$ lenne, ami nem eleme. Így ez egy kommutatív gyűrű.

   (d) $\langle \{f(x) : \ x \in \mathbb{R}\}, \{+, \circ\} \rangle$ – valós függvények összeadásra és kompozícióra
   Az összeadás Abel-csoportsága nyilvánvaló (azért ellenőrizendő!); nullelem az $x \to 0$

függvény. A kompozíciót érdemes részletesebben megnézni. A zártság triviális (két függvény kompozíciója is függvény), az asszociativitás teljesül, hiszen $(f(x)\circ g(x))\circ h(x) = g(f(x))\circ h(x) = h(g(f(x)))$, valamint $f(x)\circ(g(x)\circ h(x)) = f(x)\circ h(g(x)) = h(g(f(x)))$. Az egységelem az $x \to x$ függvény, hiszen $x \circ f(x) = f(x)$. Az inverzzel problémák vannak, mert minden $f(x)$ függvényhez léteznie kéne olyan f^{-1} függvénynek, hogy $f(x) \circ f^{-1}(x) = x$, amit csak az invertálható függvények tudnak. A kommutativitás nyilván nem teljesül, hiszen pl $x^2 \circ \sin(x) = \sin(x^2)$, míg $\sin(x) \circ x^2 = \sin^2(x) \neq \sin(x^2)$. A disztributivitás nem teljesül, mert pl $f(x) = x^2$, $g(x) = x^2$, $h(x) = x^2$ esetén $(f(x)+g(x))\circ h(x) = h(f(x)+g(x)) = (x^2+x^2)^2 = 4x^4$, míg $f(x)\circ h(x)+g(x)\circ h(x) = h(f(x)) + h(g(x)) = (x^2)^2 + (x^2)^2 = 2x^4 \neq 4x^4$, így még csak nem is gyűrűnk van.

---

8. **Csoportot alkotnak-e az alábbi H halmazok a megadott műveletekre?**

   (a) $H = \mathbb{R}$ **a valós számok halmaza, a művelet pedig a hagyományos szorzás.**
   A szorzás művelet, az asszociativitás rendben, egységelem az 1, de sajnos a 0-nak nincs inverze, így csak félcsoport.

   (b) $H = \mathbb{R} \setminus \{0\}$**, ahol $\mathbb{R}$ a valós számok halmaza, a művelet pedig a következő:** $a * b = 2ab$**, ahol a jobboldalon a hagyományos szorzás szerepel.**
   A műveletség stimmel, az asszociativitás ellenőrzése:

$$(a * b) * c = (2ab) * c = 4abc = a * (2bc) = a * (b * c),$$

   tehát rendben. Egységelem $\frac{1}{2}$, hiszen $a*\frac{1}{2} = 2a\frac{1}{2} = a$. Inverz $\frac{1}{4a}$, hiszen $a*\frac{1}{4a} = 2a\frac{1}{4a} = \frac{1}{2}$, és mivel a nem 0, ezért mindenkinek tényleg van inverze. Tehát csoport, sőt, Abel-csoport.

   (c) $H = \{2k+1 : k \in \mathbb{Z}\}$**, a művelet pedig az összeadás.**
   Két páratlan szám összege páros, így az összeadás még csak nem is művelet.

   (d) $H = \{2k : k \in \mathbb{Z}\}$**, a művelet pedig a szorzás.**
   Két páros szám szorzata páros, így művelet, valamint az asszociativitás is rendben van, így félcsoport. Több nem lehet, mert az egységelemmel és az inverzzel is komoly bajok vannak.

   (e) $H = \{2k+1 : k \in \mathbb{Z}\}$**, a művelet pedig a szorzás.**
   Lásd mint előbb, az egységelemmel már nincs baj, de inverz még mindig nincs.

   (f) H **a** $\pmod m$ **szerint vett teljes maradékrendszer (**$H = \{0, 1, \ldots m-1\}$**), a művelet pedig a maradékosztályokon értelmezett összeadás.**
   Abel-csoport, hiszen művelet, asszociatív, kommutatív, egységelem a 0, inverz pedig $-a \pmod m$.

9. **Legyen G olyan csoport, ahol $a^2 = e$ teljesül minden $a \in G$ elemre. Bizonyítsuk be, hogy G Abel-csoport!**
   Tfh nem Abel-csoport, azaz létezik olyan $a, b \in G$, hogy $ab \neq ba$. Ekkor

$$\begin{aligned} ab &\neq ba \\ aab &\neq aba \\ aabb &\neq abab \\ (aa)(bb) &\neq (ab)(ab) \\ a^2b^2 &\neq (ab)^2 \\ ee &\neq e \\ e &\neq e \end{aligned}$$

   ami nyilván lehetetlen.

10. **Egy G csoportban minden $a, b \in G$ elempárra teljesül, hogy $(ab)^{-1} = a^{-1}b^{-1}$. Bizonyítsuk be, hogy ekkor G Abel-csoport!**
Tfh nem Abel-csoport, azaz létezik olyan $a, b \in G$, hogy $ab \neq ba$. Ekkor

$$\begin{aligned} ab &\neq ba \\ ab(ba)^{-1} &\neq (ba)(ba)^{-1} \\ abb^{-1}a^{-1} &\neq e \\ aa^{-1} &\neq e \\ e &\neq e \end{aligned}$$

ami nyilván lehetetlen.

11. **Legyen $(G_1, *) \leq (G, *)$ és $(G_2, *) \leq (G, *)$ a $(G, *)$ csoport két részcsoportja! Részcsoportok-e: $(G_1 \cap G_2, *)$, $(G_1 \cup G_2, *)$?**
$(G_1 \cap G_2, *)$: az asszociativitás nem romlik el, valamint az egységelem is nyilván benne van. A zártság rendben van, hiszen ha bármely $g, h \in G_1 \cap G_2$, akkor $g * h \in G_1$ (hiszen csoport), valamint $g * h \in G_2$ ugyanezért, tehát $g * h \in G_1 \cap G_2$. Az inverz hasonlóan rendben van, hiszen bármely $g \in G_1 \cap G_2$ esetén $g^{-1} \in G_1$ (mert csoport), továbbá $g^{-1} \in G_2$ ugyanezért, tehát $g^{-1} \in G_1 \cap G_2$. Vagyis a csoportsághoz mindent igazoltunk.
$(G_1 \cup G_2, *)$: nézzük $\mathbb{Z}_6^+$ két részcsoportját: $(\{0, 2, 4\}, +)$, valamint $(\{0, 3\}, +)$. Ekkor ennek kéne csoportnak lennie: $(\{0, 2, 3, 4\}, +)$. Itt viszont $2 + 3 = 5 \notin \{0, 2, 3, 4\}$, vagyis a zártság nem teljesül, tehát ez egy ellenpélda, vagyis ez nem részcsoport az eredeti csoportban.

12. **A valós számsorozatok halmaza csoportot alkot a számsorozatok összeadására nézve, mint műveletre. Az alábbi részhalmazok közül melyek alkotnak részcsoportot ebben a csoportban?**

    (a) **a konvergens számsorozatok halmaza,**
    Két konvergens sorozat összege konvergens, továbbá az azonosan 0 sorozat is konvergens, valamint egy konvergens sorozat -1-szerese is konvergens, tehát részcsoport.

    (b) **a divergens számsorozatok halmaza,**
    Az azonosan 0 sorozat nem divergens, tehát nincs benne az egységelem, tehát nem részcsoport.

    (c) **a korlátos számsorozatok halmaza,**
    Két korlátos sorozat összege korlátos, továbbá az azonosan 0 sorozat is korlátos, valamint egy korlátos sorozat -1-szerese is korlátos, tehát részcsoport.

    (d) **a monoton növő számsorozatok halmaza.**
    Létezik olyan monoton növő sorozat, amit -1-gyel szorozva nem monoton növőt kapunk (pl az $a_i = i$ is ilyen), így inverz nincs, tehát nem részcsoport.

13. **Bizonyítsuk be, hogy tetszőleges csoportban $o(gh) = o(hg)$ tetszőleges g-re és h-ra!**
Tfh nem igaz, azaz $\exists g, h \in G$, hogy $o(gh) \neq o(hg)$. Tfh $o(gh) = x, o(hg) = y$, valamint az általánosságot nem sértve $x > y > 0$. Ekkor

$$\begin{aligned} (gh)^x &= e \\ (gh)(gh)\dots(gh) &= e \\ g(hg)(hg)\dots(hg)h &= e \\ g(hg)^{x-1}h &= e \\ g(hg)^y(hg)^{x-y-1}h &= e \\ g(hg)^{x-y-1}h &= e \\ (gh)^{x-y} &= e \end{aligned}$$

vagyis $o(gh) \leq x - y$, ami ellentmond a feltételnek.

14. R **egy nullosztómentes gyűrű. Bizonyítsuk be, hogy**
(Bár ezt mindenki tudja, azért leírom: egy a elem nullosztója b, ha $a \neq 0$, $b \neq 0$, de $ab = 0$. Egy nullosztómentes gyűrűben semelyik elemnek nem lehet nullosztója.)

   (a) **ha** $a^2 = a$ **valamilyen** $a \in R$**-re, akkor** $a \in \{0, 1\}$
   Tfh nem igaz, vagyis $\exists a \notin \{0, 1\}$, hogy $a^2 = a$. Ekkor (kihasználva az ellentett létét, valamint a disztributivitást):

$$\begin{aligned} a^2 &= a \\ a^2 - a &= 0 \\ a(a-1) &= 0 \end{aligned}$$

   Ez azt jelenti, hogy a nem 0 a-nak találtunk $a-1$ személyében egy nullosztót, hiszen $a-1 \neq 0$, mert $a \neq 1$. Nullosztó pedig a feltétel szerint nem létezhet, vagyis ellentmondásra jutottunk, vagyis $a \in \{0, 1\}$.

   (b) **ha** $a^k = 0$ **valamilyen** $a \in R$**-re, akkor** $a = 0$
   Tfh $a \neq 0$, és mégis $a^k = 0$. Feltehetjük, hogy k a legkisebb hatvány, amire ez teljesül, hiszen ebben az esetben $a^{k+1} = a^{k+2} = \cdots = 0$ is igaz. Tudjuk továbbá, hogy $k > 1$, mert különben $a = 0$ lenne. Ekkor viszont bontsuk fel így:

$$aa^{k-1} = 0.$$

   Ez azt jelenti, hogy a^{k-1} személyében (ami k fentebb részletezett tulajdonságai miatt $\neq 0$) találtunk a-hoz egy nullosztót, ami lehetetlen, vagyis $a = 0$.

15. **Gyorshatványozással számítsuk ki** $7^{19} \pmod 5$ **értékét!**
$19 = 10011_b = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$.
7 hatványai: $7^{2^0} \equiv 2 \pmod 5, 7^{2^1} \equiv 7^{2^0} \cdot 7^{2^0} \equiv 4 \pmod 5, 7^{2^2} \equiv 7^{2^1} \cdot 7^{2^1} \equiv 1 \pmod 5, 7^{2^3} \equiv 7^{2^2} \cdot 7^{2^2} \equiv 1 \pmod 5, 7^{2^4} \equiv 7^{2^3} \cdot 7^{2^3} \equiv 1 \pmod 5$.
Így $7^{19} \equiv 1 \cdot 2 \cdot 4 \equiv 3 \pmod 5$.

16. **Az órán tanult prímtesztelés segítségével bizonyítsuk be, hogy 8 összetett szám, és 7 valószínűleg prím! Aki szeret sokat számolni, az 561-ről (ami összetett szám, és egyébként a legkisebb Carmichael szám) azt is beláthatja, hogy a módszer szerint valószínűleg prím!**
8: sorsolunk a-t, ez legyen 3. Ekkor $(3, 8) = 1$ (tehát 3 nem leleplező), így kiszámoljuk $3^7 \pmod 8$-at. $3^7 \equiv 3 \not\equiv 1 \pmod 8$, vagyis 3 8 árulója, azaz 8 összetett. (Ha mondjuk 4-et választottunk volna, $(4, 8) = 4$ miatt 4 leleplező lett volna.)

   7: megint mondjuk a 3 lett az első sorsolt szám, $(3, 7) = 1$, eddig jók vagyunk. $3^6 \equiv 1 \pmod 7$, tehát a 3 segítségével 7 prímségére tippelhetünk. Választunk tehát egy következő számot, ez legyen 6. $(6, 7) = 1$, eddig jó, $6^6 \equiv 1 \pmod 7$, tehát erősödik a gyanú, hogy 7 prím. Ha már elég erős a gyanúnk, akkor megállunk, és 7-et prímnek mondjuk. Ha nem elég erős a gyanúnk, akkor még próbálkozunk.

   561: az első sorsolt szám a 40. $(561, 40) = 1$, $40^{560} \equiv 1 \pmod{561}$. Tehát 561-ről azt gyanítjuk, hogy prím (40 tehát cinkosa). A következő szám mondjuk 46. $(561, 46) = 1$, $46^{560} \equiv 1 \pmod{561}$, tehát ő is cinkos. Ha nem sorsolunk 3-mal, 11-gyel, vagy 17-tel osztható számot, akkor csak cinkosokat találunk, így 561-ről azt hihetjük, hogy prím. Persze ha mondjuk a következő sorsolt szám a 30, akkor $(30, 561) = 3$, vagyis lelepleztük, hogy 561 mégis összetett.

17. **Egy közbeszerzési pályázat eredményhirdetése előtt néhány nappal a döntőbizottságban ülő egyik politikus emailt küldött egyik, megfigyelt ismerősének, melynek tárgya:** `Re: Mi lesz az eredmény?`**. Úgy tűnik, hogy politikusunk és ismerősi köre a szokásosnál tájékozottabb, így hallottak már a titkosításról. Szerencsére az elméleti hátterét a dolognak nem ismerik eléggé, ezért az ismerős nyilvános kulcsa** $(85, 43)$**, ráadásul úgy tűnik, hogy a szöveg karakterenként van titkosítva. Igazságügyi szakértőként a mi feladatunk, hogy megtudjuk, lehet-e vádat emelni az említett emberek ellen. Az üzenetben a következő számokat látjuk: 58, 48, 27, 3, 6, 48, 67, 76, 38. A (titkosítatlan) karakterkódolás az alábbi táblázat szerint történik:**

A	2	B	3	C	4	D	6	E	7	F	8	G	11	H	12	I	13
J	21	K	22	L	23	M	26	N	27	O	28	P	31	Q	32	R	33
S	36	T	37	U	38	V	41	W	42	X	43	Y	46	Z	47		48

Az üzenet megfejtéséhez ismernünk kell kedves politikusközeli vállalkozónk titkos kulcsát. Ezt vagy ellopjuk, vagy megpróbáljuk kiszámolni. Ha utóbbi mellett döntünk, akkor az $n = 85$-öt kell prímtényezőkre bontani, és innen ki tudjuk számolni a nyilvános kulcs ismeretében a titkosat. $85 = 5 \cdot 17$, tehát $p = 5$, $q = 17$, ebből $m = 4 \cdot 16 = 64$. Vagyis a következő egyenletet kell megoldani:

$$\begin{aligned} ed &\equiv 1 \pmod{m} \\ 43d &\equiv 1 \pmod{64} \\ 43d &\equiv 129 \pmod{64} \\ d &\equiv 3 \pmod{64} \end{aligned}$$

Vagyis a titkos kulcs $(85, 3)$. Innen már könnyű visszafejteni az üzenetet:

Szám	képlet	kódolatlan szám	betű
58	$58^3 \pmod{85}$	37	`T`
48	$48^3 \pmod{85}$	7	`E`
27	$27^3 \pmod{85}$	48	
3	$3^3 \pmod{85}$	27	`N`
6	$6^3 \pmod{85}$	46	`Y`
48	$48^3 \pmod{85}$	7	`E`
67	$67^3 \pmod{85}$	33	`R`
76	$76^3 \pmod{85}$	36	`S`
38	$38^3 \pmod{85}$	47	`Z`

Persze elítélni nem fogják egyiket se...

---

18. Igény szerint kérdések feltevése a gyakvezérnek, pl. email segítségével.

19. Tanulás. Megértés.

20. ???

21. Profit! (Jól sikerült vizsga. Öröm.)

Hasznos tudnivalók

- $(G, *)$ félcsoport, ha $*$ G-n zárt és asszociatív.
- $(G, *)$ csoport, ha félcsoport, $\exists\ e$ egységelem és $\forall g \in G\ \exists\ g^{-1}$ inverz.

- $(G, *)$ Abel-csoport, ha csoport és $*$ kommutatív.
- g elem által generált (ciklikus) csoport: $\langle g \rangle = \{e, g, g^2, g^3, \cdots\}$
- Lagrange: ha $H \leq G$, akkor $|H| \mid |G|$, ahol G egy csoport.
- $\langle G, \{+, \cdot\} \rangle$ gyűrű, ha $(G, +)$ Abel-csoport, $(G, \cdot)$ félcsoport, valamint teljesülnek a disztributív tulajdonságok: $a \cdot (b+c) = a \cdot b + a \cdot c$ és $(a+b) \cdot c = a \cdot c + b \cdot c$ $(\forall a, b, c \in G)$. Jelölések: $e_+ = 0$, $e_\cdot = 1$ (ha létezik), $g_+^{-1} = -g$.
- $\langle G, \{+, \cdot\} \rangle$ kommutatív gyűrű, ha gyűrű, és $\cdot$ kommutatív (vagyis $(G, \cdot)$ Abel-félcsoport).
- $\langle G, \{+, \cdot\} \rangle$ integritási tartomány, ha kommutatív gyűrű, és nullosztómentes.
- $\langle G, \{+, \cdot\} \rangle$ ferdetest, ha gyűrű, és $(G \setminus \{0\}, \cdot)$ csoport.
- $\langle G, \{+, \cdot\} \rangle$ test, ha ferdetest, és $\cdot$ kommutatív.
- RSA: p, q prímek (választjuk), $n = pq$, $m = \varphi(n) = (p-1)(q-1)$, $1 \leq e \leq n$ úgy, hogy $(e, m) = 1$ (választjuk), d-hez megoldjuk $ed \equiv 1 \mod m$-et. Nyilvános kulcs: (n, e), titkos kulcs: (n, d). Kódolófüggvény: $f(X) = X^e \mod n$, dekódolófüggvény: $f^{-1}(Y) = Y^d \mod n$.