Jegyzetek

Előszó

1. Edward Frenkel, *Don't Let Economists and Politicians Hack Your Math*, Slate, February 8, 2013, http://slate.me/128ygaM

1. fejezet. Egy varázslatos bestia

1. A kép forrása: Physics World, http://www.hk/phy.org/index2.html
2. A kép forrása: Horváth Árpád.

2. fejezet. A szimmetria lényege

1. Ebben a gondolatmenetben a „valamely tárgy szimmetriája" kifejezést olyan transzformáció megjelölésére használjuk, amely nem változtatja meg a tárgyat. Például, ha megforgatunk egy asztalt. A „valamely tárgy szimmetriája" kifejezést nem használjuk annak a tulajdonságnak a megjelölésére, hogy az adott tárgy szimmetrikus.

2. Ha az óramutató járása szerinti forgatásokat használjuk, ugyanazokhoz a forgatásokhoz jutunk: az óramutató járása szerinti 90 fokos forgatás megegyezik az óramutató járásával ellentétes, 270 fokos forgatással, stb. Megállapodás alapján a matematikusok rendszerint az óramutató járásával ellentétes forgatásokat használják, ez azonban csupán választás kérdése.

3. Ez feleslegesnek látszhat, mégsem csupán pedantériáról van szó. Ha következetesek akarunk lenni, akkor feltétlenül szükség van erre. Azt mondtuk, hogy a szimmetria olyan transzformáció, amely megőrzi az adott tárgyat. Az identikus leképezés is egy ezek közül.

A félreértések elkerülése érdekében hangsúlyozni akarom, hogy ebben a gondolatmenetben csak az adott szimmetria végső tulajdonságával törődünk. Az nem számít, hogy menet közben mi történik az adott tárggyal, csak az számít, hogy az adott tárgy pontjai végezetül hová kerülnek. Például, ha egy asztalt 360 fokkal elforgatunk, akkor az asztal összes pontja végül is a kiinduló helyzetébe fog visszakerülni. Emiatt számunkra a 360 fokos forgatás ugyanaz a szimmetria, mintha egyáltalán nem forgattuk volna. Ugyanezen ok miatt, az óramutató járásával ellentétes, 90 fokos forgatás ugyanaz, mint az óramutató járásával megegyező, 270 fokos forgatás. Egy másik példa: tegyük fel, hogy az asztalt a padlón 10 lábbal eltoljuk valamely irányban, majd visszatoljuk 10 lábbal, vagy pedig elvisszük egy másik szobába, majd visszahozzuk. Mindaddig, amíg ugyanabba a helyzetbe kerül vissza, és minden egyes pontja ugyanazt a helyet foglalja el, mint kezdetben, az így adódó szimmetriát az identikus szimmetriával azonosnak tekintjük.

4. Fontos tulajdonsága a szimmetriák kompozíciójának az ún. *asszociativitás*: ha adott három szimmetria – S, S' és S'' – akkor ezeket két különböző sorrendben végrehajtva – $(S \circ S') \circ S''$ és $S \circ (S' \circ S'')$ – ugyanaz az eredmény adódik. Ez a tulajdonság a csoportok definíciójában mint további axióma szerepel. A könyv fő részében ezt nem említettük külön, mert az ott tekintett csoportok esetén ez a tulajdonság nyilvánvalóan fennáll.

5. Amikor egy négyzet alakú asztal szimmetriáiról beszéltünk, kényelmes volt számunkra a négy szimmetriát az asztal négy sarkával azonosítani. Ugyanakkor ez az azonosítás függ attól, hogy az egyik sarkot hogyan választjuk meg – azt, amelyik az identikus szimmetriát reprezentálja. Ha ezt már megválasztottuk, akkor már valóban minden egyes szimmetriát azonosíthatunk azzal a sarokkal, amelyikbe ezt az elsőnek megválasztott sarkot átviszi az adott szimmetria. Ennek hátránya, hogy ha egy másik sarkot választunk ki arra a szerepre, hogy az identikus szimmetriát reprezentálja, akkor az előzőtől különböző azonosítást kapunk. Ezért célszerűbb megkülönböztetni az asztal szimmetriáit és az asztal pontjait.

6. Lásd Sean Carrol, *The Particle at the End of the Universe. How the Hunt for the Higgs Boson Leads Us to the Edge of a New World*, Dutton, 2012.

7. 1872-ben, a nagy hatású erlangeni programjában alkalmazta kiindulópontként a matematikus Félix Klein azt a gondolatot, hogy a formákat meghatározzák a szimmetriatulajdonságaik – eszerint tetszőleges geometria esetén a lényeges tulajdonságokat egy szimmetriacsoport határozza meg. Például az euklideszi geometria esetén a szimmetriacsoport az euklideszi tér összes olyan transzformációjából áll, amely megőrzi a távolsá-

got. Ezek a transzformációk forgatások és eltolások kompozíciói. Nemeuklideszi geometriák más szimmetriacsoportoknak felelnek meg. Ez lehetővé teszi a lehetséges geometriák osztályozását a hozzájuk tartozó szimmetriacsoportok osztályozása segítségével.

8. Ez nem azt akarja mondani, hogy egy matematikai állítás semmilyen vonatkozásban sem lehet interpretáció tárgya: például az olyan kérdések, hogy egy adott állítás mennyire fontos, milyen széles körben alkalmazható, mennyire befolyásolta a matematika fejlődését stb., lehetnek vita tárgyai. Azonban az állítás *értelme* – hogy pontosan mit is mond – nem interpretáció kérdése, feltéve, ha az állítás logikailag konzisztens. (Az állítás logikai ellentmondás-mentessége nem vita tárgya, ha egyszer megválasztottuk azt az axiómarendszert, amelyben az állítást megfogalmaztuk.)

9. Vegyük észre, hogy minden egyes forgatás tetszőleges kör alakú tárgy – pl. a kerek asztal – szimmetriatranszformációja is egyben. Ezért elvben beszélhetnénk a forgatáscsoportnak a sík helyett a kerek asztal szimmetriatranszformációi által meghatározott reprezentációjáról is. Ugyanakkor a matematikában a „reprezentáció" fogalmát speciálisan arra az esetre tartjuk fenn, amikor az adott csoport elemei az n-dimenziós euklideszi tér szimmetriáihoz vezetnek. Ezek a szimmetriák szükségszerűen megegyeznek azokkal, amelyeket a matematikusok lineáris transzformációknak neveznek. A 14. fejezet 2. jegyzete fejti ki ezt a fogalmat.

10. A forgatáscsoport tetszőleges g eleme esetén az n-dimenziós tér megfelelő szimmetriáját jelölje S_g. Ez tetszőleges g esetén szükségképpen lineáris transzformáció, továbbá a következő tulajdonságoknak kell teljesülniük: először is, a csoport tetszőleges két eleme, g és h esetén, az $S_{g\cdot h}$ szimmetria meg kell egyezzen az S_g és S_h szimmetriák kompozíciójával. Másodszor, a csoport egységelemének megfelelő szimmetria a tér identikus szimmetriája kell legyen.

11. A későbbiekben felfedezték, hogy van még további három kvark – ezek neve c-kvark, t-kvark, illetve b-kvark –, továbbá a megfelelő antikvarkjaik.

3. fejezet. Az ötödik probléma

1. Marina Roshában is volt egy kicsiny, félhivatalos zsinagóga. A *pereszt-rojka* után javult a helyzet, mivel Moszkában és más városokban egyre több zsinagóga és zsidó közösségi központ nyílt meg.

2. Mark Saul, *Kerozinka: An episode in the history of Soviet mathematics*, Notices of the American Mathematical Society, vol. 46., November, 1999, p. 1217–1220. Online elérhetőség:
http://www.ams.org/notices/199910/fea-saul.pdf

3. George G. Szpiro, *Bella Abramovna Subbotovskaya and the „Jewish People's University"*, Notices of the American Mathematical Society, vol. 54., November 2007, p. 1326–1330. Online elérhetőség:
http://www.ams.org/notices/200710/tx071001326.pdf

4. Alexander Shen az *Entrance examination to the Mech-Mat* című cikkében felsorolt néhány olyan feladatot, melyeket meg kellett oldaniuk az Moszkvai Állami Egyetemre felvételiző zsidó hallgatóknak. (Mathematical Intelligencer, vol. 16., No. 4., 1994, p. 6–10.) Ez a cikk szerepel a *You Failed Your Math Test, Comrade Einstein* című könyvben is (szerk. M. Shifman). (World Scientific, 2005) Ez a könyv a Lomonoszov Egyetem felvételi vizsgájával kapcsolatosan további cikkeket is tartalmaz, pl. I. Vardi és A. Vershik cikkét. Online elérhetőség:
http://www.ftpi.umn.edu/shifman/Comradeeinstein.pdf.

A feladatok egy másik listája megtalálható T. Khovanova és A. Radul, *Jewish Problems* című könyvében. Online elérhetőség:
http://arxiv.org/abs/1110.1556.

5. George G. Szpiro, ibid.

4. fejezet. A Kerozinka

1. Mark Saul, ibid.

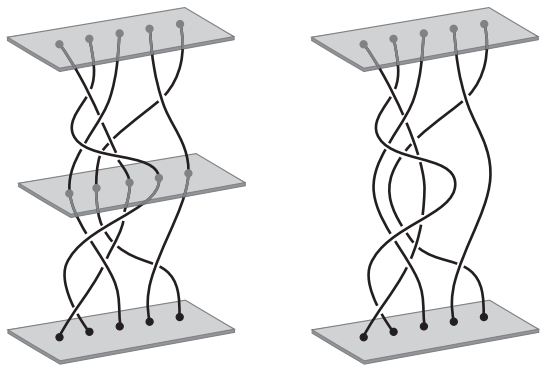
5. fejezet. A megoldás fonata

1. A Zsidó Népi Egyetem története és Bella Mucsnyik Szubbotovszkaja halálának körülményei megtalálhatóak D. B. Fuchs és mások cikkeiben is. M. Shifman (ed.), *You Failed Your Math Test, Comrade Einstein*, World Scientific, 2005.

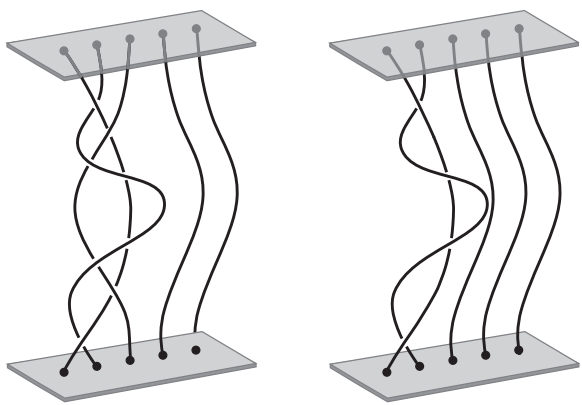
Lásd még George G. Szpiro, ibid.

2. Ha az identitásfonatot egy másik fonat tetejére helyezzük és eltávolítjuk a középső lemezt, akkor a fonalak megrövidítése után visszakapjuk az eredeti fonatot, azaz egy tetszőleges b fonat és az identitásfonat összeadása megegyezik magával a b fonattal.

3. Az ábra bemutatja, hogy mi lesz egy fonat és tükörképe összeadásának eredménye:

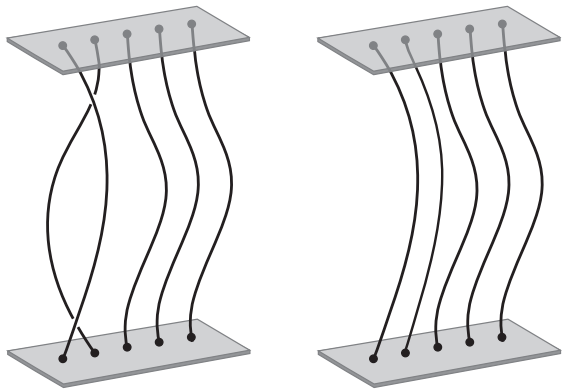


Most a fenti kép jobb oldalán szereplő fonatban húzzuk jobb oldalra azt a fonalat, amelyik a jobb szélső „szögnél" kezdődik és végződik. Az eredményt a lenti bal oldali fonat mutatja. Ezután tegyük ugyanezt a harmadik szögnél kezdődő és végződő fonallal. Ekkor a jobb oldali fonat adódik.



Ezek után húzzuk balra a második szögnél kezdődő és végződő fonalat. Az így kapott fonatban látszólag keresztezi egymást az első és a második fonal. Ez azonban csak látszólagos: a második fonalat jobbra húzva, eltűnik az

átfedés. Ezeket a mozgásokat mutatja a következő ábra. Az eredményként kapott fonat, melyet a lenti ábra jobb oldalán láthatunk, nem más, mint az identitásfonat, melyet már fent láthattunk. Pontosabban, ahhoz, hogy megkapjuk az identitásfonatot, ki kell feszítenünk a fonalakat. Szabályaink ezt lehetővé teszik (meg is kell rövidítenünk a fonalakat, hogy a kapott fonat ugyanolyan magas legyen, mint az eredeti volt). Vegyük észre, hogy egyik lépésben sem vágjuk el vagy csomózzuk össze a fonalakat, és nem engedjük meg, hogy az egyik a másikon menjen keresztül.



4. Ez jó lehetőség arra, hogy a „definíció" és a „tétel" közötti különbségre rámutassunk. A második fejezetben definiáltuk a csoportot. Eszerint a csoport olyan halmaz, melyen egy olyan műveletet is értelmeztünk (a körülményektől függően szokás ezt kompozíciónak, összeadásnak vagy szorzásnak nevezni), amely rendelkezik a következő tulajdonságokkal (vagy axiómákkal): a halmaz tartalmaz egy egységelemet (a 2. fejezetben kifejtett értelemben), továbbá minden elemnek van inverze, és a művelet eleget tesz a asszociativitás tulajdonságának, melyet a 2. fejezet 4. jegyzetében már leírtunk. Ha megadtuk ezt a definíciót, akkor ezzel a csoport fogalma egyszer és mindenkorra le van rögzítve. Semmiféle változtatást nem hajthatunk végre rajta.

Ha most adott egy halmaz, akkor megkísérelhetjük csoportstruktúrával ellátni. Ez azt jelenti, hogy valamilyen műveletet definiálunk a halmazon, és megmutatjuk, hogy ez a művelet rendelkezik a fent felsorolt tulajdonságokkal. Ebben a fejezetben az n fonallal rendelkező összes fonatot tekintettük

(azokat a fonatokat, melyek egymásból csavarással keletkeznek, azonosnak vettük, amint ezt a könyvben kifejtettük), és bevezettük két fonat összeadásának műveletét a megadott szabályok szerint. A *tételünk* az az állítás, hogy ez a művelet rendelkezik a fenti tulajdonságokkal. A tétel bizonyítása ezen tulajdonságok közvetlen ellenőrzése. Az első két tulajdonságot ellenőriztük már (lásd a fenti 2. és 3. megjegyzést), az utolsó tulajdonság (az asszociativitás) azonnal adódik abból, ahogy két fonat összeadását megkonstruáltuk.

5. Mivel szabályaink alapján a fonat saját magával nem csomózodhat össze, az egyetlen fonálból álló fonat esetén a fonálnak nincs más lehetősége, mint hogy a fenti lemez egyetlen szögéből egyenesen menjen a lenti lemez egyetlen szögéhez. Ugyanakkor akármilyen bonyolult útvonal mentén haladhat, például akár egy kanyargó hegyi ösvény vagy kígyózó út mentén is. Azonban – ha szükséges – lerövidítve elérhetjük, hogy a fonal függőlegesen lefelé tartson. Más szavakkal, a B_1 csoport egyetlenegy elemet tartalmaz, amely az egységelem (ez egyben saját maga inverze, és a saját magával való összeadás eredménye is).

6. Matematikai zsargonnal azt mondhatjuk, hogy a „B_2 fonatcsoport izomorf az egészek csoportjával". Ez azt jelenti, hogy a két csoport elemei között létezik olyan kölcsönesen egyértelmű megfeleltetés – minden egyes fonathoz hozzárendeljük az átfedések számát –, hogy a fonatok összeadása (a fent leírt értelemben) megfelel az egész számok szokásos összeadásának. Valóban, két fonatot egymás tetejére helyezve olyan új fonatot kapunk, melyben az átfedések száma megegyezik a két kiinduló fonathoz hozzárendelt számok összegével. Továbbá, az identitásfonat, amelyben egyetlen átfedés sem fordul elő, a 0 egész számnak felel meg, végezetül az inverz fonat megfelel annak, hogy az egész szám ellentettjét vesszük.

7. Lásd David Gerber, *Braid group cryptography*. *Braids: Introductory Lectures on Braids, configurations and Their Applications*, szerk. A. Jon Berrick, e. a., p. 329–403„ World Scientific, 2010. Online elérhetőség: http://arxiv.org/pdf/0711.3941v2.pdf.

8. Lásd pl. Graham P. Collins, *Computing with Quantum Knots*, Scientific American, April 2006, p. 57–63.

9. De Witt Sumners, Claus Ernst, Sylvia J. Spengler és Nicholas R. Cozzarelli, *Analysis of the mechanism of DNA recombination using tangles*, Quarterly Reviews of Biophysics, vol. 28., August 1995, p. 253–313.

Mariel Vazquez and De Witt Sumners, *Tangle analysis of Gin recombination*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 136., 2004, p. 565–582.

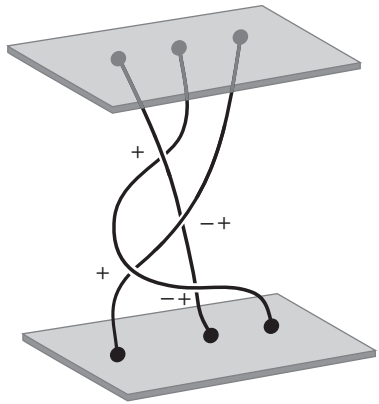
10. Valamivel pontosabb állítás – ezt a 9. fejezetben tárgyaljuk majd –, hogy a B_n fonatcsoport a sík rendezetlen, különböző pontokat tartalmazó pont n-eseinek *fundamentális csoportja*. A sík rendezetlen, különböző pontokat tartalmazó pont n-esei n-ed fokú polinomok segítségével is megadhatóak – amint azt a következő hasznos gondolatmenet mutatja. Tekintsünk egy másodfokú, 1 főegyütthatós polinomot – $x^2 + a_1x + a_2$ –, ahol a_1 és a_2 komplex számok (az „1 főegyütthatós" itt azt jelenti, hogy a x-ben legmagasabb fokú tag, azaz az x^2 együtthatója 1). Ennek két gyöke van, melyek komplex számok. Megfordítva, ezek a gyökök egyértelműen meghatározzák a másodfokú, 1 főegyütthatós polinomot. A komplex számokat tekinthetjük úgy, mint a sík pontjait (lásd 9. fejezet). Ezért a két különböző gyökkel rendelkező másodfokú, 1 főegyütthatós polinom ugyanaz, mint a sík különböző pontjait tartalmazó pontpárja.

Ehhez hasonlóan, egy n különböző komplex gyökkel rendelkező n-ed fokú, 1 főegyütthatós polinom – $x^n + a_{n-1}x^{n-1} + ...a_1x + a_0$ – megegyezik a sík egy n különböző pontból álló halmazával, a gyökei halmazával. Rögzítsünk egy ilyen polinomot: $(x-1)(x-2)...(x-n)$, melynek gyökei $1, 2, \ldots, n$. Az összes ilyen polinom terében futó görbe, amely az $(x-1)(x-2)...(x-n)$ polinomnál kezdődik és végződik, elképzelhető úgy is, mint n fonalból álló fonat: az egyes fonalak az egyes gyökök által bejárt utak. Így tehát megállapíthatjuk, hogy a B_n fonatcsoport nem más, mint a különböző gyökökkel rendelkező n-ed fokú polinomok fundamentális csoportja (lásd a 14. fejezetet).

11. A fonalak közötti átfedéshez $+1$-et rendelünk, ha a balról lefelé jövő fonál a jobbról lefelé jövő fonál alatt megy át, és -1-et rendelünk a fordított esetben. Tekintsük például a következő oldal ábráján látható fonatot!

Ha összeadjuk ezeket az egyes átfedésekhez tartozó számokat ($+1$ és -1), megkapjuk a fonat teljes átfedésszámát. Ha megcsavarjuk a fonalakat, akkor mindig ugyanolyan számú $+1$-et adunk hozzá vagy veszünk el, mint ahány -1-et, ezért a teljes átfedési szám változatlan marad. Ez azt jelenti, hogy a teljes átfedési szám *jól definiált*: nem változik meg, ha megcsavarjuk a fonatot.

12. Vegyük észre, hogy két fonat összeadása esetén a teljes átfedési szám a két fonat teljes átfedési számának összege lesz. Ezért, ha olyan fonatokat adunk össze, melyek teljes átfedési száma 0, akkor ismét olyan fonatot ka-



punk, melynek 0 a teljes átfedési száma. A $B_n^{'}$ kommutátor részcsoport ezekből a fonatokból áll. Pontosan is megfogalmazható értelemben ez a B_n fonatcsoport maximális nem-abeli része.

13. A Betti-számok fogalma a topológiából származik, amely a geometriai alakzatok lényeges tulajdonságait tanulmányozza matematikai eszközökkel. Egy adott geometriai alakzat, mint például a kör vagy a gömb, Betti-számai számsorozatot alkotnak – $b_0, b_1, b_2, \ldots$ – melyek mindegyike vagy 0, vagy természetes szám. Például valamely lapos halmaz esetén, mint pl. az egyenes vagy a sík, $b_0 = 1$, a többi Betti-szám értéke 0. Általánosan b_0 a geometriai alakzat összefüggő komponenseinek számát adja. Kör esetén $b_0 = 1, b_1 = 1$, a többi Betti-szám értéke 0. Ebben az esetben b_1 azt tükrözi vissza, hogy nemtriviális egydimenziós része van az alakzatnak. Gömb esetén $b_0 = 1, b_1 = 0, b_2 = 1$, a többi Betti-szám értéke 0. Itt b_2 értéke azt tükrözi vissza, hogy nemtriviális kétdimenziós része van az alakzatnak.

A B_n fonatcsoport Betti-számait az n különböző gyökkel rendelkező n-ed fokú, 1 főegyütthatós polinomok terének Betti-számaiként definiáljuk. A $B_n^{'}$ kommutátor részcsoport Betti-számait egy ezzel szorosan összefüggő tér Betti-számai adják. Ez azon n-ed fokú, különböző gyökökkel rendelkező 1 főegyütthatós polinomok halmaza, melyek azzal a további tulajdonsággal is rendelkeznek, hogy a diszkriminánsuk (a gyökök összes különbségei szorzatának négyzete) valamely rögzített nem nulla értéket vesz fel (pl. feltehetjük, hogy ez az érték 1). Például, az $x^2 + a_1 x + a_0$ polinom diszkriminánsa $a_1^2 - 4a_0$. Ehhez hasonló képlet adható tetszőleges n esetén.

A diszkrimináns definíciójából következik, hogy értéke pontosan akkor 0, ha a polinomnak többszörös gyökei vannak. Tehát a diszkrimináns olyan leképezést ad meg, amely a különböző gyökökkel rendelkező n-ed fokú, 1 főegyütthatós polinomokat leképezi az origó nélküli komplex síkra. Azaz ezen tér „fibrálását" kaptuk az origótól megfosztott komplex sík felett. $B_n^{'}$ Betti-számai a fibrumok topológiáját tükrözik vissza (topologikusan ezek ugyanazok), ugyanakkor B_n Betti-számai a teljes tér topológiáját tükrözik. Az a vágy, hogy megértsük a fibrált terek topológiáját, motiválta Varcsenkót, hogy elsőként ezt a problémát javasolja nekem. A Betti-számokkal és az ezzel összefüggő homológia és kohomológia fogalmával kapcsolatos további ismeretekért érdemes az alábbi bevezető tankönyveket tanulmányozni:

William Fulton, *Algebraic Topology: A First Course*, Springer, 1995.

Allen Hatcher, *Algebric Topology*, Cambridge University Press, 2001.

6. fejezet. A matematikustanonc

1. Egyesek azt gondolják, hogy Fermat talán blöffölt, amikor azt a megjegyzést a margóra feljegyezte. Én nem így gondolom. Szerintem egyszerűen csak tévedett. Mindegy, hálásaknak kell lennünk neki – ez a kis, margóra írt megjegyzés határozottan pozitív hatással volt a matematika fejlődésére.

2. Pontosabban, bebizonyítottam, hogy az n tetszőleges d osztója esetén a q-adik Betti-szám, ahol $q = n(d-2)/d$ pontosan $\phi(d)$, továbbá, hogy az $n-1$ mindegyik d osztója esetén a q-adik Betti-szám, ahol $q = (n-1)(d-2)/d$ pontosan $\phi(d)$. $B_n^{'}$ minden további Betti-száma 0-val egyenlő.

3. 1985-ben Mihail Gorbacsov került hatalomra, és nem sokkal ezután útjára indította az új irányvonalat. Ez a *peresztrojka*. Én úgy tudom, hogy az a fajta szisztematikus diszkrimináció, melyben tapasztalatom szerint a zsidó származású jelentkezők részesültek a Moszkvai Állami Egyetem felvételi vizsgája során, 1990 körül véget ért.

4. S. Zdravkovska és P. Duren, *Golden Years of Moscow Mathematics*, American Mathematical Society, 1993, p. 221.

5. Julij Iljasenko matematikus a *The black 20 years at Mech-Mat* című interjújában azt fejtette ki, hogy ez a esemény indította el a zsidóellenes irányvonalat. Ezt a cikket a Polit.ru weboldal publikálta 2009. július 28-án.

http://www.polit.ru/article/2009/07/28/ilyashenko2

6. Az volt a kérdés, hogy hányféleképpen lehet egy reguláris, $4n$ oldalú sokszög éleit párosával összeragasztani úgy, hogy olyan Riemann-felületet

kapjunk, melynek génusza n. A 9. fejezetben mutatunk erre egy speciális eljárást, amikor a sokszög átellenes éleit azonosítjuk.

7. Edward Frenkel, *Cohomology of the commutator subgroup of the braid group*, Functional Analysis and Applications, vol. 22., 1988, p. 248–250.

7. fejezet. A Nagy Egyesített Elmélet

1. A *Mathematics Newsletter* számára Robert Langlands-szal készített interjú. University of British Columbia (2010). A teljes változat elérhető az alábbi címen: http://www.math.ubc.ca/Dept/Newsletters/Robert_Langlands_interview_2010.pdf

2. Tegyük fel, hogy létezik két olyan m és n egész szám, melyekre $\sqrt{2} = m/n$. Feltehetjük, hogy m és n relatív prímek, azaz nincsen az 1-től különböző közös osztójuk. Egyébként $m = dm'$ és $n = dn'$ adódnék, és ekkor $\sqrt{2} = m'/n'$. Ezt addig lehetne ismételni, ha szükséges, ameddig két olyan számot nem kapunk, melyek már relatív prímek.

Tehát tegyük fel, hogy $\sqrt{2} = m/n$, ahol m és n relatív prímek. Négyzetre emelve a $\sqrt{2} = m/n$ képlet mindkét oldalát kapjuk, hogy $2 = m^2/n^2$. Mindkét oldalt n^2-tel megszorozva kapjuk, hogy $m^2 = 2n^2$. Ebből következik, hogy m páros szám. Ugyanis, ha páratlan lenne, akkor m^2 is az lenne, amely ellentmondana a fenti képletnek.

Ha most m páros, akkor $m = 2p$ valamely p természetes szám esetén. Behelyettesítve ezt az előző képletbe, kapjuk, hogy $4p^2 = 2n^2$, ezért $n^2 = 2p^2$. Azonban most n szintén páros szám kell legyen, ugyanazon okfejtés alapján, melynek segítségével megmutattuk, hogy m páros. Azaz, m és n is páros számok. Ez azonban ellentmond annak a feltevésnek, hogy relatív prímek. Tehát ilyen m és n szám nem létezik.

Ez jó példája az „indirekt bizonyításnak". Azzal az állítással kezdjük, amelyik éppen ellenkezője annak, amit bizonyítani próbálunk (ebben az esetben azzal az állítással, hogy $\sqrt{2}$ racionális szám, ami éppen az ellenkezője annak, amit bizonyítani akarunk). Ha ebből hamis állítás következik (esetünkben az, hogy m és n páros számok, annak ellenére, hogy feltettük, hogy relatív prímek), akkor arra következtethetünk, hogy a kiinduló állítás szintén hamis. Tehát az az állítás, amit be akartunk bizonyítani (azaz, hogy $\sqrt{2}$ nem racionális szám), igaz. Ezt az eljárást használjuk majd a 8. fejezetben is: először akkor, amikor a nagy Fermat-tétel bizonyítását elemezzük, majd a 6. számú jegyzetben akkor, amikor Eukleidész bizonyítását közöljük végtelen sok prím létezésére.

3. Például szorozzuk össze a következő két számot: $\frac{1}{2}+\sqrt{2}$ és $3-\sqrt{2}$. Egyszerűen felbontjuk a zárójeleket:

$$\left(\frac{1}{2}+\sqrt{2}\right)(3-\sqrt{2})=\frac{1}{2}\cdot 3-\frac{1}{2}\cdot\sqrt{2}+\sqrt{2}\cdot 3-\sqrt{2}\cdot\sqrt{2}\,.$$

Azonban $\sqrt{2}\cdot\sqrt{2}=2$, ezért ezeket a tagokat összegyűjtve a következő választ kapjuk:

$$\frac{3}{2}-\frac{1}{2}\sqrt{2}+3\sqrt{2}-2=-\frac{1}{2}+\frac{5}{2}\sqrt{2}\,.$$

Ez ismét ugyanilyen alakú szám, ezért ez is az új számrendszerünk eleme.

4. Az új számrendszerünknek csak olyan szimmetriáit tekintjük, amelyek kompatibilisek az összeadással és a szorzással, továbbá, amelyek során a 0 nullába megy, az 1 az 1-be, az additív inverz az additív inverzbe, a multiplikatív inverz a multiplikatív inverzbe. Azonban, ha az 1 az 1-be megy, akkor a $2=1+1$ szükségképpen az $1+1=2$-be megy. Hasonlóképpen, mindegyik természetes szám képe önmaga lesz, ezért ennek ellentettje is és multiplikatív inverze is. Ezért tehát az ilyen szimmetria minden racionális számot megőriz.

5. Könnyű ellenőrizni, hogy ez a szimmetria valóban kompatibilis az összeadással, kivonással, szorzással és osztással. Tekintsük például az összeadás műveletét. Vegyünk két különböző számot az új számrendszerünkből:

$$x+y\sqrt{2}\quad\text{és}\quad x'+y'\sqrt{2},$$

ahol x, y, x', y' racionális számok. Adjuk össze őket:

$$(x+y\sqrt{2})+(x'+y'\sqrt{2})=(x+x')+(y+y')\sqrt{2}\,.$$

Alkalmazhatjuk a tekintett szimmetriát. Ebből

$$x-y\sqrt{2}\quad\text{és}\quad x'-y'\sqrt{2}$$

adódik. Adjuk ezeket össze:

$$(x-y\sqrt{2})+(x'-y'\sqrt{2})=(x+x')-(y+y')\sqrt{2}\,.$$

Láthatjuk, hogy a kapott szám megegyezik azzal a számmal, amit a szimmetriának az eredeti összegre való alkalmazásával kapnánk:

$$(x+x')+(y+y')\sqrt{2}\to(x+x')-(y+y')\sqrt{2}\,.$$

Más szóval, külön is alkalmazhatjuk a két számra a szimmetriát, és aztán adjuk össze őket. Vagy előbb összeadjuk őket, és aztán alkalmazzuk a szimmetriát. Az eredmény ugyanaz lesz. Pontosan ez jelenti azt, hogy a szimmetriánk *kompatibilis* az összeadás műveletével. Hasonlóképpen ellenőrizhető, hogy a szimmetriánk kompatibilis a szorzás, a kivonás és az osztás műveletével is.

6. Például abban az esetben, amikor a számtestet a racionális számok $\sqrt{2}$-vel történő bővítésével kapjuk, a Galois-csoport két szimmetriából áll: az identitásból, illetve a $\sqrt{2}$-nek $-\sqrt{2}$-re való cseréléséből. Írjuk le expliciten, hogy mi adódik ezen szimmetriák kompozíciójából:

$$I \circ I = I, \quad I \circ S = S, \quad S \circ I = S,$$

és a legérdekesebb:

$$S \circ S = I\,.$$

Valóban, ha megcseréljük az $\sqrt{2}$ és a $-\sqrt{2}$ számokat, és ezt újra végrehajtjuk, akkor a nettó végeredmény az identitás lesz:

$$x + y\sqrt{2} \;\to\; x - y\sqrt{2} \;\to\; x - (-y\sqrt{2}) = x + y\sqrt{2}\,.$$

Ezzel teljesen leírtuk ezen számtest Galois-csoportját: két elemet tartalmaz – I és S –, és ezek kompozícióját a fenti formulák definiálják.

7. Néhány évvel korábban, Niels Henrik Abel megmutatta, hogy létezik olyan ötödfokú egyenlet, amelyet nem lehet megoldani gyökvonásokkal. (Joseph-Louis Lagrange és Paolo Ruffini is fontos eredményeket ért el ezen a téren.) Galois bizonyítása azonban általánosabb volt és újszerűbb elveket tartalmazott. További részletek találhatóak a Galois-csoportokkal és a magasabb fokú egyenletek megoldásának gazdag történetével kapcsolatban Mario Livio, *The Equation That Couldn't Be Solved* című könyvében (Simon és Schuster, 2005).

8. Általánosabban, tekintsük az $ax^2 + bx + c = 0$ másodfokú egyenletet, melyben a, b, c racionális számok. Ennek x_1 és x_2 megoldását a következő képlet adja meg:

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{és} \quad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}\,.$$

Ha a $b^2 - 4ac$ diszkrimináns nem valamely racionális szám négyzete, akkor ezek a megoldások nem racionális számok. Ezért, ha az x_1 és x_2 számokkal kibővítjük a racionális számokat, akkor új számtestet kapunk. Ezen számtest szimmetriacsoportja szintén két elemet tartalmaz: az identitást és a két

megoldás – x_1 és x_2 – felcseréléséből adódó szimmetriát. Más szavakkal, ez a szimmetria felcseréli a $\sqrt{b^2-4ac}$ és $-\sqrt{b^2-4ac}$ számokat.

A Galois-csoport megadásához azonban nincsen szükség arra, hogy expliciten megadjuk a megoldásokat. Valóban, mivel a vizsgált polinom foka 2, ezért tudjuk, hogy két megoldás van, tehát jelölje őket x_1 és x_2. Ekkor adódik, hogy

$$ax^2+bx+c=a(x-x_1)(x-x_2)\,.$$

Felbontva a zárójelet, kapjuk, hogy $x_1+x_2=-\frac{b}{a}$, így tehát $x_2=-\frac{b}{a}-x_1$. Ugyanakkor $(x_1)^2=-\frac{c+bx_1}{a}$, mivel x_1 megoldása a fenti egyenletnek. Ezért, ha a diszkrimináns nem négyzete valamely racionális számnak, akkor az a számtest, melyet racionális számok bővítésével kapunk úgy, hogy hozzávesszük az x_1 és x_2 számokat, az $\alpha+\beta x_1$ alakú számokból fog állni, ahol α és β racionális számok. Az x_1 és x_2 számokat felcserélő szimmetria esetén az $\alpha+\beta x_1$ szám az

$$\alpha+\beta x_2=\left(\alpha-\beta\frac{b}{a}\right)-\beta x_1$$

értékbe megy át. Ez a szimmetria kompatibilis az összeadással, stb., mert x_1 és x_2 ugyanazon racionális együtthatós egyenlet gyökei. Azt kapjuk tehát, hogy ezen számtest Galois-csoportja az indentitásból és az x_1 és x_2 értékeket felcserélő szimmetriából áll. Még egyszer hangsúlyozom, hogy semmiféle információt nem használtunk fel arra vonatkozóan, hogy az x_1 és x_2 megoldásokat hogyan lehet felírni a,b,c segítségével.

9. Szemléltetésül tekintsük például az $x^3=2$ egyenletet. Az egyik megoldás 2 köbgyöke, azaz $\sqrt[3]{2}$. Két további megoldás is van, ezek komplex számok: $\sqrt[3]{2}\omega$ és $\sqrt[3]{2}\omega^2$, ahol

$$\omega=\frac{1}{2}+\frac{\sqrt{3}}{2}\sqrt{-1}$$

(lásd a 9. fejezet komplex számokról szóló részét). Az a legkisebb számtest, amely tartalmazza mindhárom megoldást, ezek négyzeteit is tartalmazza: $\sqrt[3]{4}=\left(\sqrt[3]{2}\right)^2$, $\sqrt[3]{4}\omega$ és $\sqrt[3]{4}\omega^2$, illetve ezek hányadosát: ω és ω^2. Úgy tűnik tehát, hogy ezen számtest megkonstruálásához 8 további számot kell a racionális számokhoz hozzávenni. Teljesül azonban az alábbi összefüggés:

$$1+\omega+\omega^2=0\,,$$

amely lehetővé teszi, hogy ω^2 értékét kifejezzük 1 és ω segítségével:

$$\omega^2=-1-\omega\,.$$

Ezért tehát:

$$\sqrt[3]{2}\omega^2 = -\sqrt[3]{2} - \sqrt[3]{2}\omega, \quad \sqrt[3]{4}\omega^2 = -\sqrt[3]{4} - \sqrt[3]{4}\omega\,.$$

Tehát ahhoz, hogy megkapjuk a keresett számtestet, csak 5 új számot kell hozzávenni a racionális számokhoz: az ω, $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{4}$ és $\sqrt[3]{4}\omega$ számokat. Ezért az adódó számtest – melyet a $x^3 = 2$ egyenlet felbontási testének nevezük – tetszőleges eleme felírható hat tag kombinációjaként: racionális szám plusz racionális számszor ω plusz racionális számszor $\sqrt[3]{2}$ és így tovább. Vessük össze ezt az $x^2 = 2$ egyenlet felbontási testével, amelynek elemei két tagot tartalmaznak: racionális szám plusz racionális számszor $\sqrt{2}$.

Láttuk, hogy az $x^2 = 2$ egyenlet felbontási testéhez tartozó Galois-csoport elemei az egyenlet két gyökét – $\sqrt{2}$ és $-\sqrt{2}$ – permutálják. Két ilyen permutáció van, az egyik felcseréli ezt a két megoldást, a másik az identitás.

Ehhez hasonlóan, tetszőleges racionális együtthatós egyenlet esetén úgy definiáljuk a hozzá tartozó felbontási testet, hogy a racionális számokhoz hozzávesszük az egyenlet összes gyökét. A 4. megjegyzéshez hasonlóan az így kapott számtest tetszőleges szimmetriája, amely kompatibilis az összeadással és a szorzással, megőrzi a racionális számokat. Ezért az ilyen szimmetriák során az egyenlet tetszőleges megoldása egy másik megoldásba kell hogy átmenjen. Tehát ezen megoldások permutációit kapjuk. Az $x^3 = 2$ egyenlet esetén a fent felsorolt három megoldás van. Minden egyes permutáció esetén az első, $\sqrt[3]{2}$ ezen megoldások valamelyikébe megy át, a második, $\sqrt[3]{2}\omega$ a megmaradó két megoldás valamelyikébe, végül a harmadik, $\sqrt[3]{2}\omega^2$ szükségképpen a megmaradó megoldásba megy át (tetszőleges permutáció kölcsönösen egyértelmű kell legyen ahhoz, hogy létezzék inverze). Ezért összesen $3 \cdot 2 = 6$ lehetséges permutációja van ezen három megoldásnak. Ezek a permutációk csoportot alkotnak, és megmutatható, hogy ez a csoport kölcsösen egyértelmű megfeleltetésben áll az $x^3 = 2$ egyenlet felbontási testének Galois-csoportjával. Azaz a Galois-csoport explicit leírását kaptuk meg a megoldások permutációinak formájában.

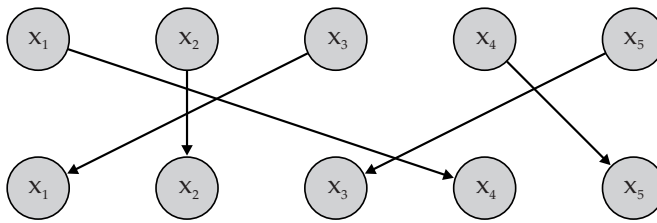
A fenti számolásban az egyenlet gyökeit expliciten megadó képleteket használtunk. De hasonló gondolatmenet alkalmazható tetszőleges, racionális együtthatós harmadfokú egyenlet esetén is, nincsen szükség olyan képletre, amely megadja az együtthatók függvényében a gyököket. Az eredmény a következő: jelölje x_1, x_2 és x_3 az egyenlet gyökeit. Tegyük fel, hogy mindegyik irracionális. Ugyanakkor könnyen látható, hogy az egyenlet diszkriminánsa, azaz

$$(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

mindig racionális szám. Megmutatható, hogy ha ennek négyzetgyöke nem racionális szám, akkor az egyenlet felbontási testének Galois-csoportja megegyezik ezen gyökök permutációiból álló csoporttal (ekkor ez 6 elemet tartalmaz). Ha a diszkrimináns négyzetgyöke racionális, akkor a Galois-csoport három permutációt tartalmaz: az identitást, az $x_1 \to x_2 \to x_3 \to x_1$ ciklikus permutációt és ennek inverzét.

10. Például nem nehéz megmutatni, hogy tipikus ötödfokú egyenlet esetén ($n = 5$), amikor is 5 gyök van, a Galois-csoport ezen öt szám permutációinak csoportja. A permutáció ezen számok kölcsönösen egyértelmű átrendezése. Az alábbi ábra például egy ilyen átrendezést mutat.

Ilyen permutáció esetén az x_1 megoldás az öt lehetőség akármelyikébe megy át (esetleg saját magába), azaz öt lehetséges választás van, azután x_2 a megmaradó négy megoldás akármelyikébe, x_3 a megmaradó három valamelyikébe és így tovább. Így összesen $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ permutáció van, tehát a Galois-csoport 120 elemből áll.



(n elem permutációinak csoportja, melyet n elem szimmetriacsoportjának is hívnak $n! = n \cdot (n-1) \dots 2 \cdot 1$ elemből áll.) Eltérően a másodfokú, harmadfokú és negyedfokú egyenletek Galois-csoportjától, ez nem feloldható csoport. Ezért, Galois érvelése alapján, az általános ötödfokú egyenlet megoldásait nem lehet gyökvonások segítségével felírni.

11. Elérhető az Institute for Advanced Study, Princeton weboldalán: http://publications.ias.edu/sites/default/files/weil1.pdf

12. Az ábra az Institute for Advanced Study digitális gyűjteményéből származik: http://cdm.itg.ias.edu/cdm/compoundobject/collection/coll12/id/1682/rec/1

8. fejezet. Mágikus számok

1. Robert Langlands, *Is there beauty in mathematical theories?* Lásd: *The Many Faces of Beauty*, szerk. Vittorio Hösle, University of Notre Dame Press, 2013. Online elérhetőség:

http://publications.ias.edu/sites/default/files/ND.pdf

2. A sejtésekről további információk találhatóak a következő mélyenszántó cikkben: Barry Mazur, *Conjectures*, Synthése, vol. 111., 1997, p. 197–210.

3. A nagy Fermat-tétel történetéről további érdekességek találhatóak az alábbi könyvben: Simon Singh, *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*, Anchor, 1998.

4. Lásd Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics, vol. 141., 1995, pp. 443–551.

Richard Taylor és Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics, vol. 141., 1995, 553–572.

Bebizonyították a Shimura–Taniyama–Weil-sejtést a legtipikusabb (az ún. szemistabil) esetben, melyről kiderült, hogy elegendő a nagy Fermat-tétel bizonyításához. Néhány évvel később, a sejtés kimaradt eseteit C. Breuil, B. Conrad, F. Diamond és R. Taylor igazolták.

Minthogy bebizonyították, helyesebb lenne a Shimura–Taniyama–Weil-sejtésre tételként hivatkozni. Valóban, számos matematikus „modularitási tételnek" nevezi. A régi megszokások azonban nehezen múlnak el, és néhányan, hozzám hasonlóan, még mindig a régi nevet használják. Ironikus, hogy a nagy Fermat-tételre mindig is tételként hivatkoztak, noha valójában sejtés volt. Kétségkívül ennek oka Fermat azon kijelentésének tiszteletben tartása, miszerint ő megtalálta a megoldást.

5. Ha N nem prím, akkor $N = xy$ valamely x és y természetes szám esetén, melyek értéke 1 és $N-1$ közé esik. Ekkor x nem rendelkezik mod N multiplikatív inverzzel. Más szavakkal, nem létezik olyan z természetes szám, melynek értéke 1 és $N-1$ között van, melyre

$$xz = 1 \quad \text{modulo } N\,.$$

Valóban, ha teljesülne a fenti egyenlőség, akkor mindkét oldalt megszorozva y értékével kapnánk, hogy

$$xyz = y \quad \text{modulo } N\,.$$

Azonban $xy = N$, tehát a bal oldal értéke Nz, ami azt jelenti, hogy y osztható N-nel. Ekkor azonban y nem lehet 1 és $N-1$ között.

6. Az Eukleidésznek tulajdonított bizonyítás a következőképpen szól. Az „indirekt" bizonyítás elvét alkalmazzuk. Ezt már használtuk ebben a fejezetben, amikor a nagy Fermat-tétel bizonyításáról esett szó.

Tegyük fel, hogy csak véges sok prím van: $p_1, p_2, \ldots, p_N$. Vegyük azt az A számot, melyet úgy kapunk, hogy ezeket összeszorozzuk és még egyet hozzáadunk: azaz legyen $A = p_1 p_2 \ldots p_N + 1$. Azt állítjuk, hogy A is prím. Indirekt érvelünk: ha nem prím, akkor az 1-en és saját magán kívül más számmal is osztható. Azaz A osztható a felsorolt prímek valamelyikével, mondjuk p_i-vel. Ekkor $A = 0$ modulo p_i. Ugyanakkor A definíciójából adódik, hogy $A = 1$ modulo p_i. Ellentmondásra jutottunk. Tehát A mégsem osztható saját magán és 1-en kívül más természetes számmal. Így A is prímszám.

Azonban A nyilvánvalóan nagyobb a $p_1, p_2, \ldots, p_N$ számok mindegyikénél. Ez ellentmond azon feltevésünknek, hogy csak a $p_1, p_2, \ldots, p_N$ számok a prímszámok. Tehát az a kiinduló feltevésünk, hogy csak véges sok prím van, hamis. Tehát végtelen sok prímszám van.

7. Fejtsük ezt ki részletesebben: az adott számrendszerben egy a szám multiplikatív inverze olyan b szám, melyre $a \cdot b = 1$. Tehát például a racionális számok esetén a $\frac{3}{4}$ racionális szám inverze $\frac{4}{3}$. Abban a számrendszerben, melyet most vizsgálunk, az 1 és $p-1$ között lévő a természetes szám inverze az a b természetes szám, amelynek értéke ugyanebbe a tartományba esik és amelyre

$$a \cdot b = 1 \quad \text{modulo } p\,.$$

Teljesen mindegy, hogy milyen számrendszert tekintünk, a 0 szám, azaz az additív egységelem nem rendelkezik multiplikatív inverzzel. Ezért zártuk ezt ki.

8. Álljon itt egy bizonyítás. Vegyünk egy a számot, mely 1 és $p-1$ közé esik, ahol p prímszám. Szorozzuk meg ezt a számot az összes olyan b számmal, amely ugyanebbe a tartományba esik, és vegyük az eredményt modulo p. Az eredményekből kétoszlopos táblázatot állíthatunk össze: az első oszlop a b szám, a második pedig $a \cdot b$ modulo p.

Például, ha $p = 5$ és $a = 2$, akkor a táblázat a következőképpen alakul:

1	2
2	4
3	1
4	3

Azonnal látjuk, hogy az $1, 2, 3, 4$ számok mindegyike pontosan egyszer szerepel a jobb oldali oszlopban. Azaz, amikor 2-vel szorzunk, ugyanazokat a számokat kapjuk vissza valamilyen permutált alakban. Például az 1 szám a harmadik sorban jelenik meg. Ez azt jelenti, hogy ha a 3-at megszorozzuk 2-vel, akkor 1-et kapunk modulo 5 eredményül. Más szavakkal, 3 lesz a 2 inverze, ha modulo 5 tekintjük az aritmetikát.

Ugyanez teljesül általánosan is: ha a fentihez hasonló táblázatot készítünk tetszőleges p prím és az $1, 2, \ldots, p-1$ listából választott a szám esetén, akkor az $1, 2, \ldots, p-1$ számok mindegyike pontosan egyszer fog szerepelni a jobb oldali oszlopban.

Bizonyítsuk ezt be, ismét az indirekt bizonyítás módszerét alkalmazva. Tegyük fel, hogy nem ez az eset. Ekkor az $1, 2, \ldots, p-1$ számok valamelyike kétszer fordul elő a jobb oldali oszlopban. Legyen ez a szám n. Ez azt jelenti, hogy az $1, 2, \ldots, p-1$ számok között két olyan is van – legyenek ezek c_1 és c_2 (feltehetjük, hogy $c_1 > c_2$) –, hogy

$$a \cdot c_1 = a \cdot c_2 = n \quad \text{modulo } p.$$

Azonban ekkor

$$a \cdot c_1 - a \cdot c_2 = a \cdot (c_1 - c_2) = 0 \quad \text{modulo } p.$$

Az utolsó képlet szerint $a \cdot (c_1 - c_2)$ osztható p-vel. Viszont ez lehetetlen, mivel p prím, és mind a, mind pedig $c_1 - c_2$ az $\{1, 2, \ldots, p-1\}$ halmazból származik.

Következésképp a táblázat jobb oldali oszlopában az $1, 2, \ldots, p-1$ számok mindegyike csak egyszer jelenhet meg. Azonban pontosan $p-1$ ilyen szám van, és éppen ugyanennyi számú sor van a táblázatban. Ezért az egyetlen lehetőség az, hogy mindegyik szám pontosan egyszer szerepeljen. Ekkor azonban az 1 szám is valahol szerepel a jobb oldali oszlopban. Legyen b a bal oldali oszlopban ennek megfelelő szám. Ekkor azonban

$$a \cdot b = 1 \quad \text{modulo } p.$$

Ezt akartuk bizonyítani.

9. Például eloszthatjuk a 4-et 3-mal az 5 elemű számtestben:

$$\begin{aligned} 4/3 = 4 \cdot 3^{-1} = 4 \cdot 2 &= 8 \text{ modulo } 5 \\ &= 3 \text{ modulo } 5 \end{aligned}$$

(itt kihasználtuk azt, hogy a 2 lesz a 3 multiplikatív inverze modulo 5).

10. Vegyük észre, hogy tetszőleges olyan a szám esetén, melynek abszolút értéke kisebb mint 1, teljesül, hogy

$$1 + a + a^2 + a^3 + a^4 + \cdots = \frac{1}{1-a}\,,$$

amit egyszerűen lehet igazolni, ha mindkét oldalt megszorozzuk $1 - a$-val. Felhasználva ezt az egyenlőséget, és a helyére $q + q^2$-t helyettesítve felírhatjuk a Fibonacci-számok

$$q\left(1 + (q+q^2) + (q+q^2)^2 + (q+q^2)^3 + \dots\right)$$

generátorfüggvényét

$$\frac{q}{1-q-q^2}$$

alakban. Ezek után elsőfokú tényezők szorzatára bontva az $1 - q - q^2$ mennyiséget, adódik, hogy

$$\frac{q}{1-q-q^2} = \frac{1}{\sqrt{5}}\left(\left(1 - \frac{1+\sqrt{5}}{2}q\right)^{-1} - \left(1 - \frac{1-\sqrt{5}}{2}q\right)^{-1}\right).$$

Ismét a fenti egyenlőséget használva, most $a = \frac{1\pm\sqrt{5}}{2}q$ mellett, kapjuk, hogy a generátorfüggvényben a q^n tag együtthatója (amely éppen F_n):

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Ezért tehát olyan zárt formulát találtunk az n-edik Fibonacci-számra, amely független az előzőektől.

Megjegyezzük, hogy a fenti képletben szereplő szám, $\frac{1+\sqrt{5}}{2}$ az ún. *aranymetszés*. A fenti képletből adódik, hogy az F_n/F_{n-1} hányados tart az aranymetszéshez, ahogy n értéke növekszik. Az aranymetszésről és a Fibonacci-számokról további részletek találhatók Mario Livio, *The Golden Ratio*, Broadway, 2003 könyvében.

11. Az eredmény bemutatása Richard Taylor, *Modular arithmetic driven by inherent beauty and human curiosity*, The Letter of the Institute for Advanced Study, Summer 2012, p. 6–8 könyve alapján történik. Köszönet Ken Ribet-nek hasznos megjegyzéseiért. André Weil *Dirichlet Series and Automorphic Forms*, Springer-Verlag, 1971 könyve szerint az ebben a fejezetben elemzett harmadfokú egyenletet Robert Fricks nyomán John Tate vezette be.

12. Ez a csoport egyike az $SL_2(\mathbb{Z})$ csoport ún. „kongruencia-részcsoportjainak". Ez a csoport az egész számokat tartalmazó 2×2-es mátrixokból áll, melyek determinánsa 1, azaz az olyan

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

egész számokból álló elrendezésekből, melyekben $ad - bc = 1$. A mátrixok szorzatát a megszokott képlet adja meg:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Tetszőleges q komplex számot, mely az egységkör belsejében van, fel lehet írni $e^{2\pi\tau\sqrt{-1}}$ alakban, valamely τ komplex szám mellett, melynek képzetes része pozitív: $\tau = x + y\sqrt{-1}$, ahol $y > 0$ (lásd a 15. fejezethez tartozó 12. megjegyzést). A q számot egyértelműen meghatározza τ és megfordítva. Ezért az $SL_2(\mathbb{Z})$ csoport hatását a q számon leírhatjuk a τ számon vett hatás segítségével. Ez utóbbit az alábbi képlet adja meg:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

Az $SL_2(\mathbb{Z})$ csoport (pontosabban ennek az I egységmátrixból és annak $-I$ ellentettjéből álló kételemű részcsoportja szerinti faktorcsoportja) megegyezik a körlap szimmetriacsoportjával, ha a körlapot valamely speciális nemeuklideszi metrikával látjuk el. Ez a Poincaré-féle körlapmodell. A tekintett függvény „2 súlyú" moduláris forma, ami azt jelenti, hogy invariáns a $SL_2(\mathbb{Z})$ kongruencia-részcsoportjának a körlapon tekintett fenti hatására, ha ezt a hatást korrigáljuk a $(c\tau + d)^2$ tényezővel való szorzással.

Lásd pl. Henri Darmon, *A proof of the full Shimura–Taniyama–Weil conjecture is announced*, Notices of the American Mathematical Society, vol. 46., December 1999, p. 1397–1401. Online elérhetőség:

http://www.ams.org/notices/199911/comm-darmon.pdf

13. Lars Madsen készítette ezt a képet, az ő engedélyével szerepel itt. Köszönöm, hogy egy igen hasznos beszélgetés során Ian Agol felhívta rá a figyelmemet.

14. Lásd pl. Neal Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation, vol. 49., 1987, p. 203–209;

I. Blake, G. Seroussi és N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

15. Véges sok p prímszám kivételével igaz ez általánosan is. További invariáns pár is tartozik a harmadfokú egyenlethez (az ún konduktor) és a moduláris formához (ún. szint); ezeket az invariánsokat is megőrzi a közölt megfeleltetés. Például a vizsgált harmadfokú egyenlet esetén mindkettő értéke 11. Megjegyzem, hogy az itt szereplő összes moduláris forma zérus konstans taggal rendelkezik, a q előtt álló b_1 együttható értéke 1, továbbá a többi b_n együttható értékét $n > 1$ esetén meghatározza a p prímnek megfelelő b_p együttható.

16. Tegyük fel, hogy a, b, c megoldása az $a^n + b^n = c^n$ Fermat-féle egyenletnek, ahol n páratlan prímszám. Ekkor – Yves Hellegouarch és Gerhard Frey nyomán – tekinthetjük az

$$y^2 = x(x - a^n)(x + b^n)$$

harmadfokú egyenletet. Ken Ribet (Frey javaslatát és Jean-Pierre Serre részeredményét követve) bebizonyította, hogy ez az egyenlet nem tehet eleget a Shimura–Taniyama–Weil-sejtésnek. Az $n = 4$ esettel együtt (melyet maga Fermat bizonyított) ebből már következik a nagy Fermat-tétel. Valóban, tetszőleges $n > 2$ szám felírható $n = mk$ szorzat alakjában, ahol m vagy 4 vagy páratlan prím. Ezért abból, hogy az ilyen m értékekre nincsen megoldása a Fermat-egyenletnek, következik, hogy tetszőleges $n > 2$ esetén sincsen.

17. Goro Shimura, *Yutaka Taniyama and his time. Very personal recollections*, Bulletin of London Mathematical Society, vol 21. 1989, p, 193.

18. ibid. p. 190.

19. Lásd az 1. lábjegyzetet a 1302–1303. oldalon Serge Lang, *Some history of the Shimura–Taniyama conjecture*, Notices of the American Mathematical Society, vol. 42., 1995, p. 1301–1307. cikkben, amely a sejtés gazdag történetét tárgyalja.

Online elérhetőség: http://www.ams.org/notices/199511//forum.pdf

9. fejezet. A rozetta-kő

1. *The Economist*, August 20, 1998, p. 70.

2. A könyvben szereplő képek a Riemann-felületekről a *Mathematica*® szoftver felhasználásával készültek, melynek kódját Stan Wagon kedvesen rendelkezésre bocsátotta. További részletért lásd az alábbi könyvet: Stan Wagon, *Mathematica®in Action: Problem Solving Through Visualization and Computation*, Springer-Verlag, 2010.

3. Ez nem pontos definíció, azonban megfelelő elképzelést ad a valós számokról. Pontos definíciót úgy kapunk, ha minden valós számot úgy

képzelünk el, mint racionális számok konvergens sorozatának határértékét (melyet Cauchy-sorozatnak is neveznek); például a $\sqrt{2}$ végtelen tizedes tört kifejtésének csonkításai ilyen sorozatot eredményeznek.

4. Ennek érdekében jelöljünk ki egy pontot a körön, és helyezzük el a kört az egyenesen úgy, hogy ez a kijelölt pont az egyenest a 0 pontban érintse. Ezek után görgessük a kört jobbra addig, amíg a kijelölt pont ismét nem érinti az egyenest (ez akkor fog bekövetkezni, amikor a kör egy teljes fordulatot megtett). A kör és az egyenes ezen érintkezési pontja felel meg a 2π-nek.

5. A komplex számok (és más számrendszerek) geometriáját szépen magyarázza Barry Mazur, *Imagining Number*, Picador, 2004 könyve.

6. Pontosabban, megkapjuk a fánk felületét egyetlen pontot kivéve. Ez az extra pont felel meg a „végtelen megoldásnak", amikor is mind x, mind pedig y végtelenhez tart.

7. Ahhoz, hogy g génusszal rendelkező Riemann-felületet kapjunk, x-ben $2g+1$-ed fokú polinomot kell az egyenlet jobb oldalára írni.

8. Ez a kapcsolat az algebra és a geometria között René Descartes mélyenszántó meglátása volt, melyet először a *La Géometrie* című munkájában írt le. Ez a *Discours de la Méthode* című, 1637-ben megjelent könyvének függeléke volt. E. T. Bell a következőt írja Descartes módszeréről: „És most jön módszerének igazi ereje. *Tetszőleges kívánt vagy javasolt komplexitású egyenletből induljunk ki, és ennek algebrai vagy analitikai tulajdonságait interpretáljuk geometriailag (...) Tehát az algebra és az analízis kell hogy vezessenek minket a tér és geometriája fel nem térképezett tengerén.*" (E. T. Bell, *Men of Mathematics*, Touchstone, 1986, p. 54.). Megjegyezzük, hogy Descartes módszere valós együtthatós egyenletek megoldásaira alkalmazható, ugyanakkor ebben a fejezetben a véges testek, illetve komplex számok körébe eső megoldások érdekelnek bennünket.

9. Például a 8. fejezetben megtanultuk, hogy az $y^2+y=x^3-x^2$ harmadfokú egyenletnek négy megoldása van modulo 5. Így tehát – naivan – az 5 elemű véges test felett az ennek megfelelő görbe négy pontot tartalmaz. Valójában azonban ennél sokkal gazdagabb a struktúra, mivel olyan megoldásokat is tekinthetünk, amelyek az 5 elemű véges test különböző kiterjesztéseiből veszik fel értéküket; például az $x^2=2$ egyenlet megoldásaival kibővített testből. Ezt majd a 14. fejezet 8. megjegyzésében fogjuk elemezni. Ezek a testbővítések összesen 5^n elemet tartalmaznak $n=2,3,4,\ldots$ esetén, tehát ilyen módon véges testbeli értékű megoldások hierarchiáját kapjuk.

A harmadfokú egyenleteknek megfelelő görbéket hívják „elliptikus görbéknek".

10. *The Bhagavad-gita*, Krishna tanácsai háború idején. Fordította Barbara Stoler Miller, Bantam Classic, 1986.

Érdemes megjegyezni, hogy Weil az 1930-as évek elején két évet töltött Indiában, és saját bevallása szerint hatott rá a hindu vallás.

11. Lásd pl. Noel Sheth, *Hindu Avatara and Christian Incarnation: A comparison*, Philosophy East and West, vol. 52., No. 1., p. 98–125.

12. André Weil, *Collected Papers*, vol. 1., Springer-Verlag, 1979, p. 251. (saját fordítás).

13. Ibid. p. 253. Az az ötlet, hogy ha valamely véges test felett adott egy görbe, akkor vehetjük a rajta értelmezett racionális függvényeket. Ezek a függvények két polinom hányadosai. (Megjegyezzük, hogy az ilyen függvényeknek „pólusuk" – olyan hely, ahol a függvény értéke nincs definiálva – van minden olyan pontban, ahol a nevezőben szereplő polinom értéke nulla.) Kiderül, hogy egy adott görbén értelmezett racionális függvények halmaza a racionális számok, vagy ennél általánosabb számtest halmazához hasonló tulajdonságokkal rendelkezik, hasonlóan a 8. fejezetben tárgyaltakhoz.

A pontosabb magyarázat érdekében tekintsünk Riemann-felületen értelmezett racionális függvényeket; az analógia itt szintén fennáll. Például vegyük a gömböt. Sztereografikus projekciót alkalmazva ezt a gömböt úgy is tekinthetjük, mint egy pont és a komplex sík egyesítését (az extra pontot tekinthetjük úgy, hogy az reprezentálja a végtelent). Jelölje $t = r + s\sqrt{-1}$ a komplex síkon vett koordinátát. Ekkor minden $P(t)$ komplex együtthatós polinom a síkon értelmezett függvény. Ezek a polinomok felelnek meg a számelméletben szereplő egész számoknak. A gömbön értelmezett racionális függvény két, közös tényező nélküli polinom $P(t)/Q(t)$ hányadosa. Ezek a racionális függvények analógok a racionális számokkal, melyek olyan egész számok m/n hányadosai, melyeknek nincsen közös osztójuk. Ehhez hasonlóan, általánosabb Riemann-felületen a racionális függvények analógok az általánosabb számtestek elemeivel.

Ezen analógia ereje abban rejlik, hogy számos, a számtestekről szóló eredményhez hasonló eredmény lesz igaz a véges testek felett tekintett görbék racionális függvényei esetén és megfordítva is. Néha egyszerűbb észrevenni és/vagy bizonyítani valamely állítást az egyikre. Ekkor az analógia azt sugallja nekünk, hogy ehhez hasonló állítás kell hogy igaz legyen a másikra is. Ez volt az egyik olyan eszköz, melyet Weil és más matematikusok

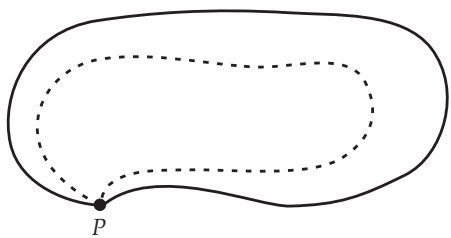
felhasználtak új eredmények elérésére.

14. Ibid. p. 253. Itt Martin H. Krieger fordítását használom. Lásd Notices of the American Mathematical Society, vol. 52., 2005, p. 340.

15. Három olyan Weil-sejtés volt, melyet Bernard Dwork, Alexander Grothendieck és Pierre Deligne bizonyított.

16. Ez a definíció redundáns. Ennek kifejtéséhez tekintsünk a síkon két görbét – amint azt az alábbi ábra mutatja –, az egyiket folytonos, a másikat pontozott vonal jelöli. Világos, hogy az egyiket a másikba át lehet alakítani folytonos deformációval anélkül, hogy szét kellene szakítani. Ésszerű és gazdaságos azt mondani, hogy két olyan zárt görbét, melyet így egymásba lehet alakítani, egyenlőnek tekintünk. Az átalakításokat végrehajtva drasztikusan lecsökkentjük a csoportunk elemeinek számát.

Ez az elv hasonló ahhoz az elvhez, melyet az 5. fejezetben a fonatcsoport definíciója során használtunk. Ott két fonatot azonosnak tekintettünk, ha egymásba lehet deformálni (vagy csavarni) őket anélkül, hogy a fonalakat elvágtuk vagy egymáson átfűztük volna.



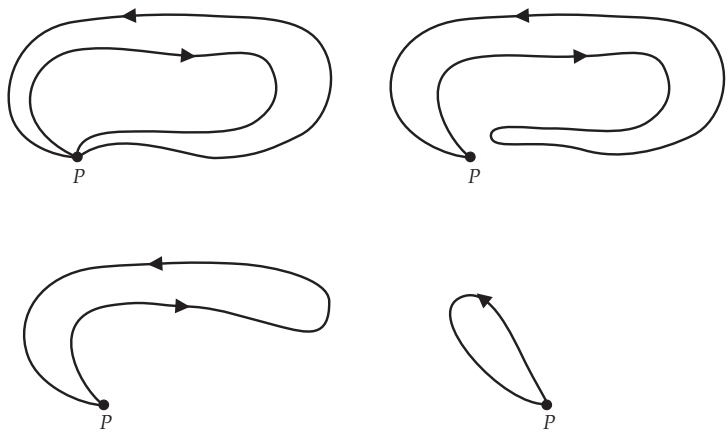
A Riemann-felület fundamentális csoportját tehát úgy definiáljuk, hogy elemei a P pontban induló és végződő zárt görbék, azzal a további megkötéssel, hogy azokat a görbéket, melyeket folytonos deformációval egymásba át lehet vinni, azonosnak tekintjük.

Jegyezzük meg, hogy ha a Riemann-felület összefüggő, s ezt hallgatólagosan mindig feltesszük, akkor a P referenciapont megválasztása lényegtelen: a különböző P referenciapontokhoz tartozó fundamentális csoportok kölcsönösen egyértelmű megfeleltetésben vannak egymással (pontosabban egymással „izomorfak" lesznek).

17. Az egységelem a „konstans" görbe. Ez soha nem hagyja el a megjelölt P pontot. Valóban, célszerű minden egyes zárt görbét úgy elképzelni, mint valamely részecske trajektóriáját, amely a P pontból indul ki és oda tér

vissza. A konstans görbe azon részecske trajektóriája, amely a P pontban marad. Világos, hogy ha tetszőleges görbét hozzáadunk a konstans görbéhez, abban az értelemben, ahogy a könyvben leírtuk, akkor az eredeti görbét kapjuk vissza.

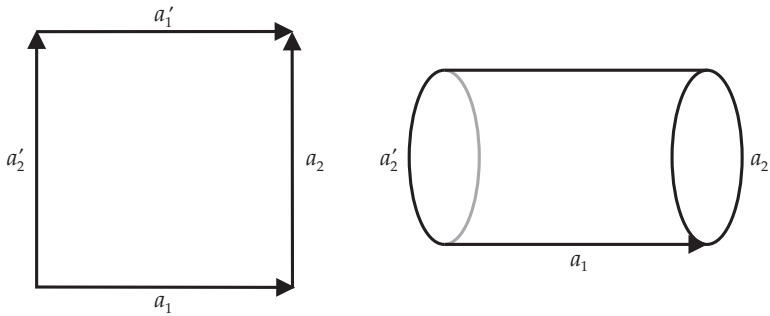
Egy adott görbe inverz görbéje ugyanaz a görbe lesz, azonban az ellenkező irányban bejárva. Ennek ellenőrzésére adjuk össze a görbét és az inverzét. Olyan új görbét kapunk, amely ugyanazon az úton kétszer megy át, de ellentétes irányban. Ezt az új „kettős" görbét folytonos deformációval a konstans görbébe alakíthatjuk át. Először is a két görbe egyikét egy kicsit csavarjuk meg. Az eredményként kapott görbe egy pontra húzható össze, amint az alábbi ábra mutatja.



18. Az 5. fejezet 10. jegyzetében megismerttől eltérően a B_n fonatcsoportot lehet úgy is interpretálni, mint az n különböző gyökkel rendelkező n-ed fokú 1 főegyütthatós polinomok terének fundamentális csoportját. A P referenciapontnak az $(x-1)(x-2)\dots(x-n)$ polinomot választjuk, melynek gyökei $1, 2, \dots, n$ (ezek a fonat „szögei").

19. Ahhoz, hogy megmutassuk, hogy a két görbe kommutál egymással, vegyük észre, hogy a tóruszt megkaphatjuk úgy, hogy egy négyzet (négycsúcsú sokszög) átellenes oldalait összeragasztjuk. Összeragasztva a két vízszintes oldalt – a_1-et és a_1'-t – hengert kapunk. A henger átellenes végein lévő köröket összeragasztva (ez lesz az első ragasztás eredményeként

a négyzet két függőleges – a_2 és a_2' – oldalából), kapjuk a tóruszt. Látjuk, hogy az a_1 és a_2 oldalak a tórusz két független zárt görbéjévé alakultak. Vegyük észre, hogy a tóruszon a négy csúcs ugyanazt a pontot adja, így tehát ezek a görbék zártak lesznek – a tórusz ugyanazon P pontjából indulnak és ott végződnek. Továbbá $a_1 = a_1'$, mivel összeragasztottuk őket, és hasonlóan $a_2 = a_2'$.



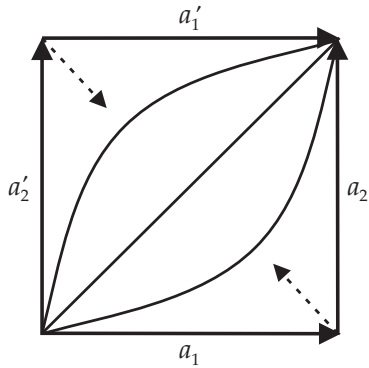
A négyzeten, ha az a_1 görbét vesszük, majd az a_2 görbét, akkor ez az egyik csúcsból az átellenes csúcsba visz át minket. Az eredményként kapott görbe $a_1 + a_2$. Azonban ezen csúcsok között más görbe mentén is haladhatunk: először vesszük az a_2' majd az a_1' görbét. Az eredményként kapott görbe $a_2' + a_1'$. A négyzet átellenes oldalait összeragasztva az a_1' görbe az a_1 lesz, az a_2' görbe az a_2. Azaz $a_2' + a_1' = a_2 + a_1$.

Vegyük észre, hogy mind $a_1 + a_2$, mind pedig $a_2 + a_1$ átalakítható a diagonális görbébe, amely két átellenes csúcsot köt össze egyenes vonallal (a szaggatott nyíl mutatja, hogyan kell deformálni ezt a két görbét).

Ez azt jelenti, hogy $a_1 + a_2$ és $a_2 + a_1$ a tórusz fundamentális csoportjának ugyanazt az elemét eredményezik. Megmutattuk, hogy

$$a_1 + a_2 = a_2 + a_1 \,.$$

Ebből következik, hogy a tórusz fundamentális csoportjának egyszerű szerkezete van: az elemei felírhatóak $M \cdot a_1 + N \cdot a_2$ alakban, ahol a_1 és a_2 a tóruszon az a két kör, melyet a 131. oldal ábráján mutattunk be, továbbá M és N egész számok. A fundamentális csoportban az összeadás megegyezik ezen kifejezések szokásos összeadásával.



20. Pozitív g génusszal (azaz g lyukkal) rendelkező Riemann-felület fundamentális csoportjának legegyszerűbb leírását kapjuk, ha ismét elképzeljük, hogy valamely sokszög átellenes éleinek összeragasztásával megkaphatjuk a felületet – azonban most $4g$ csúcsú sokszög esetén. Például ragasszuk össze egy nyolcszög (azaz 8 csúccsal rendelkező sokszög) átellenes éleit. Ebben az esetben négy darab átellenes él van, mindegyik párban azonosítjuk ezeket a oldalakat. A ragasztást nehezebb elképzelni, mint a tórusz esetében, azonban ismert, hogy ekkor olyan Riemann-felületet kapunk, melynek génusza 2 (ez az ún. dán péksütemény felülete).

Ezt a konstrukciót felhasználhatjuk arra, hogy megadjuk egy általános Riemann-felület fundamentális csoportját, hasonlóan ahhoz, ahogy ezt a tórusz fundamentális csoportja esetén tettük. A tórusz esetéhez hasonlóan a g génusszal rendelkező Riemann-felület fundamentális csoportjában $2g$ elemet konstruálunk meg azáltal, hogy a sokszög egymás után következő, $2g$ darabszámú oldala mentén tekintjük a görbéket. (A kimaradó $2g$ oldal mindegyikét ezek valamelyikével azonosítottuk.) Jelölje ezeket $a_1, a_2, \ldots, a_{2g}$. Ezek generálják a Riemann-felületünk fundamentális csoportját abban az értelemben, hogy ezen csoport mindegyik eleme megkapható úgy, hogy ezeket összeadjuk, akár többször is. Például $g = 2$ esetén szerepel a következő elem: $a_3 + 2a_1 + 3a_2 + a_3$. (Jegyezzük meg, hogy ezt nem lehet átírni $2a_3 + 2a_1 + 3a_2$ alakba, mivel a_3 nem kommutál az a_2 és a_1 elemekkel, így nem vihetjük a jobb szélső a_3 elemet a bal oldalra.)

Ugyanúgy, ahogyan a tórusz esetén, a sokszög két átellenes csúcsát összekötő görbét két különböző módon felírva, az alábbi összefüggést kapjuk,

amely a tórusz esetében adódó kommutativitás általánosítása:

$$a_1 + a_2 + \ldots a_{2g-1} + a_{2g} = a_{2g} + a_{2g-1} + \cdots + a_2 + a_1 \,.$$

Megmutatható, hogy aktuálisan ez az egyetlen összefüggés ezek között az elemek között. Így pontosan leírtuk a fundamentális csoportot: az $a_1, a_2, \ldots,$ a_{2g} elemek generálják a fenti relációnak eleget téve.

21. Pontosabban kifejtve, tekintsük a Riemann-felületen értelmezett összes racionális függvényt – a fenti 13. megjegyzés értelmében. Ezek analógok a racionális számokkal. A megfelelő Galois-csoport azon számtest szimmetriacsoportja, melyet úgy kapunk, hogy valamely polinomegyenlet, például az $x^2 = 2$ gyökeivel bővítjük a racionális számok testét. Ehhez hasonlóan, az X Riemann-felületen értelmezett racionális függvényekhez hozzávehetjük a polinomegyenletek megoldásait. Kiderül, hogy ennek során egy másik $X^{'}$ Riemann-felület racionális függvényeit kapjuk, amely „fedi" az X felületet; azaz létezik egy véges fibrummal rendelkező $X^{'} \to X$ leképezés. Ebben az esetben a Galois-csoport az $X^{'}$ olyan szimmetriáiból áll, melyek X összes pontját fixen hagyják. Más szavakkal, ezek a szimmetriák az $X^{'} \to X$ leképezés fibrumain hatnak.

Vegyük észre, hogy ha veszünk az X Riemann-felületen egy zárt görbét, amely X valamely P pontjából indul és ott végződik, akkor tekinthetjük a P pont feletti fibrum tetszőleges pontját, és „követhetjük" ezt az adott görbe mentén. Amikor visszaérünk, általában a P pont feletti fibrum másik pontjához jutunk, azaz ezen fibrum egy transzformációját kapjuk. Ez a monodrómia jelensége, melyet majd a 15. fejezetben elemzünk részletesebben. A fibrum ezen transzformációjából eljuthatunk a Galois-csoport egy eleméhez. Tehát a fundamentális csoport és a Galois-csoport között találtunk valamilyen kapcsolatot.

10. fejezet. Élet a hurokban

1. A „speciális" jelző arra utal, hogy ezek a ortogonális transzformációk megőrzik az irányítást – ezek pontosan a gömbön vett forgatások. Példa olyan ortogonális transzformációra, amely nem őrzi meg az irányítást (azaz nem eleme a $SO(3)$ csoportnak), a valamelyik koordinátasíkra való tükrözés. Az $SO(3)$ csoport szorosan összefügg az $SU(3)$ csoporttal (a 3-dimenziós tér speciális unitér csoportja). Ez utóbbit vizsgáltuk a kvarkokkal kapcsolatban a 2. fejezetben. Az $SU(3)$ csoport az $SO(3)$ csoporthoz hasonlóan definiálható; a *valós* 3-dimenziós teret fel kell cserélni a *komplex* 3-dimenziós

térre.

2. Még egy másik módon is beláthatjuk, hogy a kör egydimenziós: emlékezzünk vissza arra, hogy a kört úgy is tekinthetjük, mint az $x^2 + y^2 = 1$ egyenlet valós megoldásait; ezt vettük a 9. fejezetben. Így tehát a kör a sík azon pontjainak halmaza, melyek egyetlen egyenletnek tesznek eleget. Ezért dimenziója megegyezik a sík dimenziója – ami kettő – mínusz az egyenletek számával, tehát egy.

3. Ez az idézet szerepel Duchamp jegyzetében, melynek címe: *A l'Infinitif*, amint azt Gerald Holton, *Henri Poincaré, Marcel Duchamp and innovation in science and art*, Leonardo, vol. 34., 2001, p. 130. idézi.

4. Linda Dalrymple Henderson, *The fourth Dimension and Non-Euclidean Geomerty in Modern Art*, MIT Press, 2013, p. 493.

5. Gerald Holton, ibid. p. 134.

6. Charles Darwin, *Autobiographies*, Penguin Classics, 2002, p. 30.

7. További részletekért lásd például: Shing-Tung Yau és Steve Nadis, *The Shape of Inner Space*, Basic Books, 2010.

8. Kiderül, hogy e csoport dimenziója $n(n-1)/2$. Más szavakkal, a csoport valamely elemének leírásához $n(n-1)/2$ független koordinátára van szükség ($n = 3$ esetén $3(3-1)/2 = 3$ koordinátára, amint azt a könyv fő részében láttuk).

9. Matematikailag minden egyes hurkot tekinthetünk úgy is, mint a kör valamely „leképezését" a háromdimenziós térbe, azaz olyan szabálynak, amely a kör minden egyes ϕ pontjához a háromdimenziós tér valamely $f(\phi)$ pontját rendeli hozzá. Csak „sima" leképezéseket tekintünk. Durván szólva ez azt jelenti, hogy a hurokban nincsenek éles szögek vagy sarkok, vagyis ahhoz hasonló, amilyet a könyv fő részében lévő ábra mutat.

Általánosabban, valamely S sokaságból egy M sokaságba való leképezés nem más, mint egy olyan szabály, amely az S minden egyes s pontjához hozzárendel egy pontot az M-ből, melyet az s képének nevezünk.

10. Lásd például: Brian Greene, *The Elegant Universe*, Vintage Books, 2003.

11. Pontosabban, az $SO(3)$-beli hurok nem más, mint $SO(3)$ elemeinek valamely $\{f(\phi)\}$ gyűjteménye, melyet a ϕ szög parametrizál (ez utóbbi a körön vett koordináta). Ha adott egy másik hurok, amely a $\{g(\phi)\}$ elemek együttese, akkor tekintsük a két forgatás kompozícióját, amely $f(\phi) \circ g(\phi)$ minden egyes ϕ esetén. Ekkor egy új $\{f(\phi) \circ g(\phi)\}$ elemegyüttest kapunk, amely egy másik, $SO(3)$-beli hurok. Tehát $SO(3)$-ban vett tetszőleges hu-

rokpár esetén előállíthatunk egy harmadik hurkot. Ez a hurokcsoport szorzási szabálya. A hurokcsoport egységeleme az a hurok, amely a $SO(3)$ egységelemére koncentrálódik, azaz $F(\phi)$ az $SO(3)$ identitása minden egyes ϕ esetén. Az $\{f(\phi)\}$ hurok inverze az $\{f(\phi)^{-1}\}$ hurok. Könnyen megmutatható, hogy az összes csoportaxióma teljesül. Ezért tehát az $SO(3)$ huroktere valóban csoport.

12. Ennek igazolására vegyünk egy egyszerűbb példát: a sík hurokterét. A sík két koordinátával rendelkezik, legyenek ezek x és y. Ezért a síkon bármely hurok nem más, mint a sík pontjainak az $x(\phi)$ és $y(\phi)$ koordinátákkal rendelkező gyűjteménye minden olyan ϕ szög esetén, melynek értéke 0 és 360 fok közé esik. (Például, az $x(\phi) = \cos(\phi), y(\phi) = \sin(\phi)$ képletek speciális hurkot adnak meg: ez az 1 sugarú, origó középpontú kör.) Tehát egy ilyen hurok megadásához $(x(\phi, y(\phi))$ számpárok végtelen gyűjteményét kell megadnunk, minden egyes ϕ szög esetén egy párt. Ez az oka annak, hogy a síkon a hurkok tere végtelen dimenziós. Ugyanezen ok miatt bármely véges dimenziós sokaság esetén a hurkok tere szintén végtelen dimenziós.

13. R. E. Langer idézi a *René Descartes*, The American Mathematical Monthly, vol. 44., No. 8. October 1937, p. 508. könyvben.

14. Az érintősík az ezen a ponton átmenő összes sík közül a gömbhöz legközelebbi sík. Ez csak érinti a gömböt ebben az egy pontban. Ugyanakkor, ha bármilyen kicsit is elmozdítjuk ezt a síkot (úgy, hogy még mindig átmenjen a gömb ugyanazon rögzített pontján), olyan síkot kapunk, amely már több pontban metszi a gömböt.

15. Definíció szerint egy adott Lie-csoport Lie-algebrája az a lapos tér (mint például az egyenes, a sík és így tovább), amelyik a legközelebb van a Lie-csoporthoz az összes olyan lapos tér közül, amelyek a Lie-csoport egységelemének megfelelő ponton mennek át.

16. Egy általános kör nem tartalmaz speciális pontot. Azonban a „körcsoport" igen: ez a csoport identitáseleme, amely egy speciális pont a körön. Ahhoz, hogy a kör csoport legyen, ki kell jelölni ezt a pontot.

17. A vektortér pontosabb definíciója következik.

Ha valamely n-dimenziós lapos térben már megválasztottunk egy koordináta-rendszert, akkor ezen tér pontjait azonosíthatjuk valós számokból álló $(x_1, x_2, \ldots, x_n)$ szám n-esekkel. Az x_i számok a pont koordinátái. Ezek között létezik egy speciális pont: $(0, 0, \ldots, 0)$, melyben mindegyik koordináta értéke nulla. Ez az origó.

Rögzítsünk le most egy $(x_1, x_2, \ldots, x_n)$ pontot ebben a térben. Definiál-

juk a tér egy szimmetriáját, amely tetszőleges másik $(z_1, z_2, \ldots, z_n)$ pontot a $(z_1 + x_1, z_2 + x_2, \ldots, z_n + x_n)$ pontba visz át. Geometriailag ezt a szimmetriát úgy képzelhetjük el, hogy az n-dimenziós teret eltoljuk azon kijelölt intervallum irányában, amely az origót és az $(x_1, x_2, \ldots, x_n)$ pontokat köti össze. Jelölje ezt a vektort $< x_1, x_2, \ldots, x_n >$. Kölcsönösen egyértelmű megfeleltetés létezik az n-dimenziós lapos tér pontjai és a vektorok között. Emiatt a rögzített koordináta-rendszerrel rendelkező lapos teret a vektorok terének is tekinthetjük. Ezért *vektortér*nek nevezzük.

Hogy vektorokban gondolkodunk és nem pontokban, annak az az előnye, hogy a vektorokon két természetes művelet is van. Az első művelet a vektorok összeadása, amely a vektorok terét csoporttá alakítja. Amint azt a 2. fejezetben kifejtettük, a szimmetriákat komponálhatjuk egymással, ezért a szimmetriák csoportot alkotnak. Az előző bekezdésben leírt eltolásszimmetriák kompozíciója a vektorok következő összeadásához vezet:

$$< x_1, x_2, \ldots, x_n > + < y_1, y_2, \ldots, y_n > = < x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n > .$$

A vektorok csoportjának egységeleme a $< 0, 0, \ldots, 0 >$ vektor. Az $< x_1, x_2, \ldots, x_n >$ vektor additív inverze az $< -x_1, -x_2, \ldots, -x_n >$ vektor.

A második művelet a vektorok valós számmal való szorzása. Az $< x_1, x_2, \ldots, x_n >$ vektort a k valós számmal szorozva a $< kx_1, kx_2, \ldots, kx_n >$ vektort kapjuk.

Tehát egy vektortéren két struktúra is létezik: az összeadás, amely eleget tesz a csoporttulajdonságoknak, és a számmal való szorzás. Ezek a struktúrák természetes tulajdonságokkal kell rendelkezzenek.

Ugyanakkor az érintőtér is vektortér, ezért bármely Lie-algebra is vektortér.

Amit fent leírtunk, az a valós számok feletti vektortér. Valóban, a vektorok koordinátái valós számok, és vektorokat valós számokkal szorozhatunk. Ha a valós számokat a fenti leírásban komplex számokra cseréljük, akkor a komplex számok feletti vektortér fogalmát kapjuk.

18. A Lie-algebra ezen műveletét rendszerint szögletes zárójellel jelölik, így ha $\vec{a}$ és $\vec{b}$ egy Lie-algebra (ami egyben vektortér is, amint azt az előző megjegyzésben kifejtettük) két elemét jelöli, akkor a rajtuk végrehajtott ezen művelet eredményét $[\vec{a}, \vec{b}]$ jelöli. Ez a következő tulajdonságokkal rendelkezik: $[\vec{a}, \vec{b}] = -[\vec{b}, \vec{a}]$, $[\vec{a} + \vec{b}, \vec{c}] = [\vec{a}, \vec{c}] + [\vec{b}, \vec{c}]$, $[k\vec{a}, \vec{b}] = k[\vec{a}, \vec{b}]$, tetszőleges k szám esetén, továbbá teljesül az ún. Jacobi-azonosság:

$$[[\vec{a}, \vec{b}], \vec{c}] + [[\vec{b}, \vec{c}], \vec{a}] + [[\vec{c}, \vec{a}], \vec{b}] = 0 .$$

19. A háromdimenziós tér két vektorának – $\vec{a}$-nak és $\vec{b}$-nek – a vektoriális szorzata maga is vektor, melyet $\vec{a} \times \vec{b}$ jelöl, és amely merőleges az $\vec{a}$ és $\vec{b}$ vektorokat tartalmazó síkra, hossza megegyezik az $\vec{a}$ és $\vec{b}$ vektorok hossza és a köztük lévő szög szinuszának szorzatával, és az $\vec{a}$, $\vec{b}$ és $\vec{a} \times \vec{b}$ vektorhármas irányítása pozitív (ez az ún. jobbkéz-szabály segítségével is kifejezhető).

20. Például, az $SO(3)$ Lie-csoport Lie-algebrája a háromdimenziós vektortér. Ezért az $SO(3)$ hurokcsoportjának Lie-algebrája ezen háromdimenziós tér összes hurkából áll. A háromdimenziós tér vektoriális szorzata Lie-algebra-struktúrát ad ezeken a hurkokon. Azaz, ha adott két hurok, akkor egy harmadikat is előállíthatunk, bár szavakkal nem egyszerű leírni, hogy ez pontosan mi lesz.

21. Pontosabban a Kac–Moody-algebra a hurokcsoport Lie-algebrájának kibővítése egy egydimenziós térrel. További részleteket tartalmaz Victor Kac, *Infinite-dimensional Lie Algebras* (Third Edition, Cambridge University Press, 1990) könyve.

22. A Virasoro-algebra szimmetriával rendelkező modelleket konform térelméletnek nevezik. Ezeket először Alekszander Belavin, Alekszander Poljakov és Alekszander Zamolodcsikov orosz fizikusok vezették be 1984-ben. Nagy hatású munkájuk Feigin és Fuchs, továbbá Victor Kac eredményein alapultak.

23. Ezek közül a legismertebbek a Wess–Zumino–Witten-modellek. További részletekért lásd Edward Frenkel és David Ben-Zvi, *Vertex Algebras* (Second Edition, American Mathematical Society, 2004) munkát.

24. Ezen „kvantummezőknek" (angolul quantum fields) semmi közük sincsen a „számtestekhez" (angolul number fields) vagy a „véges testekhez" (angolul finite fields), melyeket a korábbi fejezetekben elemeztünk. Ez egy másik példa a zavaró matematikai terminológiára, ámbár más nyelveken nem lép fel ez a zavar: franciául például a „mező" szót használják a kvantummezőre, és „testet" a számtestre és a véges testre.

11. fejezet. A csúcs meghódítása

1. A pontos konstrukció: tegyük fel, hogy veszünk egy elemet az $SO(3)$ hurokcsoportjából, amely az $SO(3)$ elemeinek $\{g(\phi)\}$ együttese, melyet a ϕ parametrizál (a körön vett koordináta). Ugyanakkor a gömb hurokterének eleme a gömb $\{f(\phi)\}$ pontjainak együttese, melyet ϕ paraméterez. Adott $\{g(\phi)\}$ és $\{f(\phi)\}$ esetén tekinthetjük a gömb hurokterének egy másik elemét is mint az $\{g(\phi)\,(f(\phi))\}$ pontok együttesét. Ez azt jelenti, hogy

alkalmazzuk a $g(\phi)$ forgatást a gömb $f(\phi)$ pontjára, minden egyes ϕ esetén egymástól függetlenül. Tehát láthatjuk, hogy az $SO(3)$ hurokcsoportjának minden egyes eleme a gömb hurokcsoportjának egy szimmetriájához vezet.

2. A zászlósokaság tetszőleges pontja több elemből áll: valamely rögzített n-dimenziós tér egy egyenese, egy sík, amely tartalmazza ezt a egyenest, egy háromdimenziós tér, amely tartalmazza a síkot, stb. egészen egy $(n-1)$-dimenziós hipersíkig, amely mindegyiket tartalmazza.

Állítsuk szembe ezt a projektív terekkel, melyeket kezdetben tanulmányoztam: a projektív tér egy pontja mindössze egyetlen egyenes az n-dimenziós térben, semmi más.

A legegyszerűbb, $n = 2$ esetben, amikor a rögzített tér kétdimenziós, az egyetlen választásunk csak az egyenes (egyetlen sík van, maga a tér). Ezért ebben az esetben a zászlósokaság ugyanaz, mint a projektív tér, és kiderül, hogy egybeeesik a gömbbel. Fontos megjegyezni, hogy az egyeneseket, a síkokat és így tovább komplex térben (és nem valós térben) tekintjük, és csak azokat, amelyek átmennek a rögzített n-dimenziós tér origóján.

A következő példa $n = 3$, ekkor a háromdimenziós térrel van dolgunk. Ebben az esetben a projektív tér ezen háromdimenziós tér összes egyenesét tartalmazza, azonban a zászlósokaság párokból áll össze: egy egyenes és egy sík, amely ezt tartalmazza (csak egyetlen háromdimenziós tér van). Ezért ebben az esetben különbség van a projetív tér és a zászlósokaság között. Az egyenest tekinthetjük egy zászló rúdjának, a síkot pedig a zászló vásznának. Innen származik a „zászlósokaság" elnevezés.

3. Boris Feigin és Edward Frenkel, *A family of representations of affine Lie-algebras*, Russian Mathematical Surveys, vol. 43., No. 5., 1988, p. 221–222.

12. fejezet. A tudás fája

1. Mark Saul, *Kerozinka: An episode in the history of Soviet mathematics*, Notices of the American Mathematical Society, vol. 46., November 1999, p. 1217–1220.

2. Később megtudtam, hogy Gelfand, aki szívspecialistákkal is együttműködött (ugyanazon ok miatt, amiért Jakov Iszajevics urológusokkal), szintén sikerrel alkalmazta ezt a megközelítést az orvosi kutatásban.

14. fejezet. A bölcsesség kévéinek összerakása

1. A vektortér pontos definíciója szerepel a 10. fejezet 17. jegyzetében.

2. A vektorterek kategóriája esetében valamely V_1 vektortérből egy V_2 vektortérbe mutató morfizmusok a V_1-ből V_2-be képező lineáris transzformációk. Ezek olyan f leképezések V_1-ből V_2-be, melyekre $f(\vec{a}+\vec{b}) = f(\vec{a}) + f(\vec{b})$ tetszőleges $\vec{a}$ és $\vec{b}$ V_1-beli vektor esetén, továbbá $F(k\cdot\vec{a}) = kf(\vec{a})$ tetszőleges $\vec{a}$ V_1-beli vektor és k szám esetén. Speciálisan, valamely V vektortér saját magába ható morfizmusai a V-ből saját magába ható lineáris transzformációk. V szimmetriacsoportja azokból a morfizmusokból áll, melyeknek van inverzük.

3. Lásd például Benjamin C. Pierce, *Basic Category Theory for Computer Scientists*, MIT Press, 1991.

Joseph Goguen, *A categorical manifesto*, Mathematical Structures in Computer Science, vol. 1., 1991, p. 49–67.

Steve Awodey, *Category Theory*, Oxford University Press, 2010.

4. Lásd például http://www.haskell.org/haskellwiki/Category_theory és az ottani hivatkozásokat.

5. Lásd például Masaki Kashiwara és Pierre Schapira, *Sheaves on Manifolds*, Springer-Verlag, 2010.

6. A modulo valamely p prím szerint vett aritmetika ezen meglepő tulajdonságának egyszerű magyarázata van, ha a csoportelmélet szemszögéből nézzük. Tekintsük a véges test nem nulla elemeit: $1, 2, \ldots, p-1$. A szorzásra nézve csoportot alkotnak. Valóban, a szorzás műveletének egységeleme az 1 szám: ha egy a elemet 1-gyel megszorzunk, akkor visszakapjuk a értékét. Minden egyes elemnek van inverze, amint azt a 8. fejezet 8. jegyzetében megmagyaráztuk: tetszőleges a szám esetén, mely az $\{1, 2, \ldots, p-1\}$ halmazba esik, létezik olyan b elem, melyre $a \cdot b = 1$ modulo p. Ennek a csoportnak $p-1$ eleme van. Általánosan igaz tény, amely *tetszőleges* véges G csoport esetén teljesül, hogy ha N eleme van, akkor a csoport tetszőleges elemének az N-edik hatványa megegyezik az egységelemmel (melyet az 1 jelöl):

$$a^N = 1\,.$$

Ennek bizonyítására tekintsük a G csoport következő elemeit: $1, a, a^2, \ldots$. Mivel a G csoport véges, ezért ezek az elemek nem lehetnek mind különbözőek. Kell hogy legyenek ismétlések. Legyen k az a legkisebb természetes szám, melyre a^k vagy 1 vagy a^j valamely $j = 1, \ldots, k-1$ esetén. Tegyük fel, hogy az utóbbi eset teljesül. Legyen a^{-1} az a inverze, azaz $a\cdot a^{-1} = 1$, és vegyük ennek j-dik hatványát: $\left(a^{-1}\right)^j$. Szorozzuk meg az $a^k = a^j$ egyenlet mindkét oldalát az $\left(a^{-1}\right)^j$ mennyiséggel jobbról. Minden egyes alkalommal, ha $a \cdot a^{-1}$ adódik, akkor cseréljük ki 1-re. Az 1-gyel szorozva nem

változik meg az eredmény, így az 1 mindig eltávolítható a szorzatból. Láthatjuk tehát, hogy mindegyik a^{-1} egyet kitöröl az a-kból. Tehát a bal oldal értéke a^{k-j} lesz, a jobb oldal pedig 1-gyel egyenlő. Kapjuk, hogy $a^{k-j} = 1$. Azonban $k - j$ kisebb mint k, ez pedig ellentmond k megválasztásának. Következésképpen, a listánkban az első ismétlődés szüségképpen $a^k = 1$ alakú, így az $1, a, a^2, \ldots, a^{k-1}$ elemek mind különbözőek. Ez azt jelenti, hogy k elemből álló csoportot alkotnak: $\{1, a, a^2, \ldots, a^{k-1}\}$. Ez az N elemből álló eredeti G csoportnak részcsoportja abban az értelemben, hogy G elemeinek részhalmazából áll, és ezen részhalmaz tetszőleges két elemének szorzata ismét ennek a részhalmaznak lesz eleme, a részhalmaz tartalmazza a G csoport egységelemét, és ez a részhalmaz minden egyes elemének inverzét is tartalmazza.

Ugyanakkor ismert, hogy tetszőleges részcsoport elemeinek száma osztója a csoport elemei számának. Ezt az állítást nevezik Lagrange-tételnek. Az olvasóra hagyom a bizonyítást (vagy akár Google-n meg lehet keresni). Az $\{1, a, a^2, \ldots, a^{k-1}\}$ részcsoportra – amely k elemet tartalmaz – alkalmazva Lagrange-tételét azt kapjuk, hogy k osztója n-nek, a G csoport elemei számának. Ezért $N = km$ valamely m természetes szám esetén. Mivel $a^k = 1$, azt kapjuk, hogy

$$a^N = \left(a^k\right) \cdot \left(a^k\right) \cdot \cdots \cdot \left(a^k\right) = 1 \cdot 1 \cdot \cdots \cdot 1 = 1\,.$$

Pontosan ezt akartuk igazolni.

Térjünk vissza az $\{1, 2, \ldots, p-1\}$ csoporthoz, melyen értelmezve van a szorzás művelete. Ennek $p-1$ eleme van. Ez tehát a G csoportunk, így most N éppen $p - 1$. Alkalmazzuk az általános tételt erre a esetre. Azt kapjuk, hogy $a^{p-1} = 1$ modulo p, tetszőleges a esetén, az $\{1, 2, \ldots, p-1\}$ számok közül. Ekkor azonban

$$a^p = a \cdot a^{p-1} = a \cdot 1 = a \mod p\,.$$

Könnyen látható, hogy ez utóbbi képlet tetszőleges egész a érték esetén igaz, ha megállapodunk abban, hogy

$$x = y \mod p,$$

ha $x - y = rp$ valamely r egész szám mellett.

Ez a kis Fermat-tétel állítása. Fermat először egy barátjához írt levelében fogalmazta meg. Elküldöm majd a bizonyítást – írta –, de attól félek, túl hosszú.

7. Az eddigiekben modulo valamely p prímszám szerinti aritmetikát tekintettünk. Ugyanakkor kiderül, hogy a kis Fermat-tétellel analóg állítás teljesül bármely n természetes szám mint modulus szerint vett aritmetika esetén. Ahhoz, hogy ezt megmagyarázzuk, fel kell idéznünk az Euler-féle ϕ-függvényt, amelyet a 6. fejezetben a fonatcsoport kapcsán már elemeztünk. (A fonatcsoporttal kapcsolatos vizsgálódásaim során azt kaptam, hogy a fonatcsoport Betti-számai kifejezhetőek ezen függvény segítségével.) Emlékeztetek arra, hogy $\phi(n)$ azon 1 és $n-1$ közé eső természetes számok száma, amelyek relatív prímek n-nel, azaz amelyeknek nincsen az n-nel (1-től különböző) közös osztójuk. Például, ha n prím, akkor mindegyik 1 és $n-1$ közé eső szám relatív prím n-nel, és így $\phi(n) = n-1$.

Az $a^{p-1} = 1$ modulo p képlettel – melyet az előző jegyzetben bizonyítottunk – analóg képlet a következő:

$$a^{\phi(n)} = 1 \quad \text{modulo } n\,.$$

Ez tetszőleges n egész szám és tetszőleges olyan a természetes szám esetén fennáll, amely relatív prím n-nel. Pontosan ugyanúgy igazolható, mint az előbb: vegyük azon természetes számok halmazát 1 és $n-1$ között, melyek relatív prímek n-nel. Ebből $\phi(n)$ darab van. Könnyen megmutatható, hogy a szorzás műveletével csoportot alkotnak. Ezért Lagrange tétele alapján a csoport tetszőleges eleme esetén annak $\phi(n)$-edik hatványa az egységelem lesz.

Példaként tekintsük azt az esetet, amikor n két prím szorzata, azaz $n = pq$, ahol p és q különböző prímszámok. Ebben az esetben azok a számok, melyek nem relatív prímek n-nel, vagy p-vel, vagy q val oszthatóak. Az előzőek $p \cdot i$ alakúak, ahol $i = 1, 2, \ldots, q-1$ (ebből $q-1$ darab van), az utóbbiak pedig $q \cdot j$ alakúak, ahol $j = 1, \ldots, p-1$ (ebből $p-1$ darab van). Azt kapjuk tehát, hogy

$$\phi(n) = (n-1) - (q-1) - (p-1) = (p-1)(q-1)\,.$$

Ezért tehát

$$a^{(p-1)(q-1)} = 1 \quad \text{modulo } pq$$

tetszőleges olyan a szám esetén, amely nem osztható sem p-vel, sem q-val. Könnyű látni, hogy az

$$a^{1+m(p-1)(q-1)} = a \quad \text{modulo } pq$$

összefüggés tetszőleges a természetes szám és m egész szám esetén teljesül.

Ez az egyenlet az egyik legáltalánosabban használt titkosítási algoritmus, az ún RSA-algoritmus alapja (az elnevezés Ron Rivest, Adi Shamir és Leonard Adleman nyomán született, akik 1977-ben írták le az algoritmust). Az ötlet lényege, hogy választunk két prímet – p és q – (különféle algoritmusok léteznek ezek generálására), és legyen n a szorzatuk. Az n számot nyilvánosan közöljük, azonban a p és q prímeket nem. Ezután választunk egy e számot, amely relatív prím $(p-1)(q-1)$ értékével. Ezt a számot szintén közzétesszük.

A titkosítási eljárás tetszőleges a számot (pl. egy hitelkártyaszámot) kicserél a^e modulo n értékre.

$$a \quad \to \quad b = a^e \quad \text{modulo } n\,.$$

Megmutatható, hogy hatékonyan vissza lehet állítani a értékét az a^e szám ismeretében. Nevezetesen, keresünk egy olyan d számot 1 és $(p-1)(q-1)$ között, melyre

$$de = 1 \quad \text{modulo } (p-1)(q-1)\,.$$

Más szavakkal,

$$de = 1 + m(p-1)(q-1)$$

valamely m természetes szám esetén. Ekkor

$$\begin{aligned} a^{de} \quad \text{modulo } n \quad &= \quad a^{1+m(p-1)(q-1)} \quad \text{modulo } n \\ &= \quad a \quad \text{modulo } n \end{aligned}$$

a fenti képlet alapján.

Ezért, ha adott $b = a^e$, akkor az eredeti a számot a következőképpen kaphatjuk vissza:

$$b \quad \to \quad b^d \quad \text{modulo } n\,.$$

Foglaljuk össze: Az n és az e számokat nyilvánnossá tesszük, azonban d értékét titokban tartjuk. A titkosítást a következő képlet adja meg:

$$a \quad \to \quad b = a^e \quad \text{modulo } n\,.$$

Ezt bárki meg tudja tenni, mert e és n nyilvánosan elérhetőek.

A visszafejtést a következő képlet írja le

$$b \quad \to \quad b^d \quad \text{modulo } n\,.$$

Ezt az a^e számra alkalmazva visszakapjuk az eredeti a számot. De csak azok tudják ezt a műveletet végrehajtani, akik ismerik d értékét.

A fenti titkosítási eljárás azért jó, mert a kódolt szám visszafejtését lehetővé tevő d szám megismeréséhez ismernünk kell $(p-1)(q-1)$ értékét. Ehhez azonban tudnunk kell, hogy mi volt p és q, az n két prímosztója. p és q értéke azonban titkos. Elegendően nagy n esetén, a prímfaktorizációk ismert módszereit alkalmazva, sok-sok hónapba kerülne – még igen gyors számítógépek hálózatával is – p és q értékének meghatározása. 2009-ben kutatók egy csoportja több száz igen gyors számítógépet párhuzamosan használva, képes volt prímekre bontani egy 232 számjegyű számot: az eljárás két évet vett igénybe (lásd: http://eprint.iacr.org/2010/006.pdf). Ha azonban valaki előállna valamilyen hatékonyabb módszerrel, melynek segítségével a természetes számokat prímek szorzatára lehet bontani (például kvantumszámítógépet használva), akkor kezében van az az eszköz, melynek segítségével fel lehetne törni ezt a titkosítási sémát. Ez az oka annak, hogy intenzív kutatás folyik a számok prímfaktorokra való bontása terén.

8. Láttuk, hogy az $x^2 = 2$ alakú egyenletnek nincs megoldása a racionális számok között. Ebben az esetben egy új számrendszert hozhatunk létre a két megoldás, $\sqrt{2}$ és $-\sqrt{2}$ hozzávételével. Azt is láttuk, hogy a $\sqrt{2}$ és a $-\sqrt{2}$ felcserélése szimmetriát eredményez a számok ezen új rendszerén.

Hasonlóképpen, tekinthetjük az x változó polinomjai által megadott egyenleteket is, például az $x^2 = 2$ vagy $x^3 - x = 1$ egyenleteket mint a $\{0, 1, 2, \ldots, p-1\}$ véges testben vett egyenleteket. Ekkor megkérdezhetjük, hogy vajon az adott egyenlet x-re megoldható-e ezen véges testen belül. Ha nincsen megoldása, akkor a megoldásokat hozzávehetjük a véges testhez, ugyanúgy, ahogy a $\sqrt{2}$ és $-\sqrt{2}$ értékét hozzávettük a racionális számokhoz. Ezen a módon új számtesteket szerkeszthetünk.

Például, ha $p = 7$, akkor az $x^2 = 2$ egyenletnek két megoldása van – 3 és 4 –, mert

$$3^2 = 9 = 2 \quad \text{modulo } 7\,, \quad 4^2 = 16 = 2 \quad \text{modulo } 7\,.$$

Jegyezzük meg, hogy a 4 megegyezik a -3-mal a modulo 7 vett aritmetika szerint, mert $3 + 4 = 0$ modulo 7. Tehát ez a két megoldás egymás ellentettje, ugyanúgy, mint $\sqrt{2}$ és $-\sqrt{2}$ is egymás ellentettjei. Ez nem meglepő: Az $x^2 = 2$ egyenlet megoldásai mindig egymás ellentettjei kell legyenek, mert ha $a^2 = 2$, akkor ugyancsak $(-a)^2 = (-1)^2 a^2 = 2$. Ez azt jelenti, hogy ha $p \neq 2$, akkor a véges testben mindig két elem lesz, melyeknek ugyanaz a négyzete, és ezek egymás ellentettjei (ha $p \neq 2$, akkor p szükségképpen páratlan, és ezért $-a$ nem lehet egyenlő a-val. Egyébként p értéke megegyezne $2a$-val). Ezért az $\{1, 2, \ldots, p-1\}$ véges test elemeinek csak a fele lehet négyzetszám.

(A híres Gauss-féle reciprocitási elv leírja, hogy mely n számok négyzetszámok a modulo p vett aritmetikában, és melyek nem azok. Ez kívül esik könyvünk hatókörén, annyit azonban megjegyzünk, hogy a válasz csak p modulo $4n$ vett értékétől függ. Tehát tudjuk például, hogy $n = 2$ négyzetszám modulo $p = 7$. Ebben az esetben $4n = 8$. Tehát minden olyan p prímre n négyzetszám lesz modulo p, amely p értéke 7 modulo 8, függetlenül attól, hogy milyen nagy szám p. Megdöbbentő eredmény.)

Ha $p = 5$, akkor $1^2 = 1, 2^2 = 4, 3^2 = 4$ és $4^2 = 1$ modulo 5. Tehát 1 és 4 négyzetszámok modulo 5, azonban 2 és 3 nem. Speciálisan, látjuk, hogy az $x^2 = 2$ egyenletnek a $\{0, 1, 2, 3, 4\}$ véges testben nincsen megoldása, ugyanúgy, mint ahogyan a racionális számok esetében sem volt. Ezért egy új számrendszert hozhatunk létre a $\{0, 1, 2, 3, 4\}$ véges testnek az $x^2 = 2$ egyenlet megoldásaival történő kibővítésével. Jelölje ezeket megint $\sqrt{2}$ és $-\sqrt{2}$ (ne feledjük el, hogy ezek nem ugyanazok a számok, amelyekkel korábban a racionális számokat bővítettük).

Ezáltal olyan új számtestet kapunk, melynek elemei

$$a + b\sqrt{2}$$

alakúak, ahol a és b értéke a $\{0, 1, 2, 3, 4\}$ halmazba tartozik. Mivel két paraméterünk van – a és b –, melyek értékei $0, 1, 2, 3, 4$, ezért adódik, hogy az új számtestnek $5 \cdot 5 = 25$ eleme van. Általában, a $\{0, 1, \ldots, p-1\}$ test tetszőleges véges bővítése p^m elemet tartalmaz valamilyen m természetes szám esetén.

Tegyük fel, hogy a $\{0, 1, 2, \ldots, p-1\}$ véges számtesthez hozzávesszük az összes egyváltozós polinomegyenlet gyökeit. Ekkor egy olyan új számrendszert kapunk, melyet a véges test *algebrai lezárásá*nak nevezünk. Az eredeti véges testnek p eleme volt. Kiderül, hogy az algebrai lezárásának végtelen sok eleme van. A következő kérdésünk, hogy mi ezen algebrai lezárás Galois-csoportja. Ezek az algebrai lezárás olyan szimmetriái, melyek megőrzik az összeadás és a szorzás műveletét, és az eredeti számtest p darabszámú elemét saját magukba viszik át.

Ha a racionális számok testét vesszük kiindulásul, és ennek algebrai lezárását tekintjük, akkor az ennek megfelelő Galois-csoport igen bonyolult. A Langlands-program célja részben éppen az volt, hogy a harmonikus analízis eszközeivel leírja ezt a Galois-csoportot és ennek reprezentációit.

Ezzel ellentétben a $\{0, 1, 2, \ldots, p-1\}$ véges test algebrai lezártjának Galois-csoportja egészen egyszerűnek bizonyul. Nevezetesen, a szimmetriák egyikét már ismerjük: ez a Frobenius-szimmetria, amely a p-edik hat-

ványra való emelés $a \to a^p$ művelete. A kis Fermat-tétel alapján a Frobenius megőrzi az eredeti p elemű véges test mindegyik elemét. Ugyancsak megőrzi az összeadást és a szorzást is az algebrai lezárásban:

$$(a+b)^p = a^p + b^p\,, \quad (ab)^p = a^p b^p\,.$$

Ezért a Frobenius a véges test algebrai lezártjának Galois-csoportjához tartozik.

Jelöljük a Frobeniust F-fel. Nyilvánvaló, hogy a Frobenius tetszőleges egész hatványa – F^n – is eleme a Galois-csoportnak. Például az F^2 az a művelet, melynek során a p^2-dik hatványra emelünk: $a \to a^{p^2} = (a^p)^p$. Az F^n szimmetriák, midőn n végigfut az egész számokon, a Galois-csoportnak részcsoportját alkotják, melynek neve Weil-csoport, André Weil iránti tiszteletből. Maga a Galois-csoport a Weil-csoportnak ún. teljes lezárása, az F egész kitevős hatványain túlmenően még olyan elemeket is tartalmaz, melyek F^n bizonyos határértékei, midőn n tart a végtelenbe. Bizonyos értelemben tehát a Frobenius generálja a Galois-csoportot.

Lássunk egy példát arra, hogy a Frobenius hogyan hat egy véges test algebrai lezártjának az elemein. Tekintsük a $p = 5$ esetet, és az algebrai lezárt fenti alakú elemeit:

$$a + b\sqrt{2},$$

ahol a és b értéke $0, 1, 2, 3$ vagy 4. A számok ezen rendszerének egy szimmetriája, ha a $\sqrt{2}$ értékét kicseréljük a $-\sqrt{2}$-re.

$$a + b\sqrt{2} \quad \to \quad a - b\sqrt{2}\,,$$

ahhoz hasonlóan, mint amikor a racionális számokat bővítettük a $\sqrt{2}$-vel. Meglepő (és nincsen megfelelője a racionális számok esetén), hogy ez a felcserélési szimmetria valójában megegyezik a Frobenius-szimmetriával. Valóban, a Frobenius alkalmazása a $\sqrt{2}$-re azt jelenti, hogy az 5-dik hatványra emeljük. Adódik, hogy

$$\left(\sqrt{2}\right)^5 = \left(\sqrt{2}\right)^2 \cdot \left(\sqrt{2}\right)^2 \cdot \sqrt{2} = 2 \cdot 2 \cdot \sqrt{2} = 4 \cdot \sqrt{2} = -\sqrt{2}\,,$$

mivel $4 = -1$ modulo 5. Ebből következik, hogy $p = 5$ esetén a Frobenius az $a + b\sqrt{2}$ elemet az $a - b\sqrt{2}$ elembe viszi át. Ugyanez teljesül tetszőleges olyan p prímszám esetén, melyre az $x^2 = 2$ egyenletnek nincsen megoldása a $\{0, 1, 2, \ldots, p-1\}$ véges testben.

9. Egy n-dimenziós vektortér tetszőleges szimmetriáját – helyesebb lineáris transzformációnak nevezni (lásd a 2. jegyzetet) – mátrix segítségével

lehet reprezentálni. Ez nem más, mint az a_{ij} elemek négyzet alakban való elrendezése, ahol i és j értéke 1 és n között fut, ahol n a vektortér dimenziója. A mátrix nyoma a mátrix diagonális elemeinek összege, azaz az a_{ii} alakú elemeké, ahol i értéke 1 és n között fut.

10. A jelen szövegösszefüggésben a „visszavezetés" azt jelentené, hogy egy adott függvény esetén találjunk a sokaság felett egy olyan kévét, hogy a sokaság minden s pontjához tartozó fibrumon vett Frobenius nyoma éppen az f függvény s pontbeli értéke legyen. Tetszőleges szám előállítható egy vektortér valamely szimmetriájának nyomaként. A nehézség abban áll, hogy ezeket a vektortereket valahogy koherensen kellene összeválogatni, hogy teljesüljenek a kéve tulajdonságai.

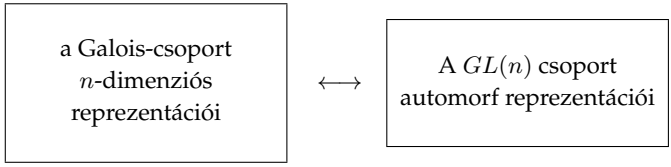
15. fejezet. Nemes keringők

1. A Galois-csoport H csoporton vett reprezentációja olyan szabály, amely a Galois-csoport minden egyes eleméhez hozzárendeli a H csoport valamely elemét. Eleget kell tegyen annak a feltételnek, hogy ha a, b a Galois-csoport két eleme és $f(a)$, $f(b)$ a hozzájuk rendelt H-beli elemek, akkor a Galois-csoportban vett $a \cdot b$ szorzat képe a H-ban az $f(a)f(b)$ szorzat legyen. Megfelelőbb elnevezés, hogy ez a Galois-csoport egy *homomorfizmusa* a H csoportba.

2. Ahhoz, hogy ezt pontosabbá tegyük, idézzük fel a 10. fejezet 17. jegyzetéből az n-dimenziós vektortér definícióját. Amint azt a 2. fejezetben elemeztük, egy adott csoport n-dimenziós reprezentációja olyan szabály, amely a csoport minden egyes g eleméhez az n-dimenziós vektortér egy S_g szimmetriáját rendeli hozzá. Ez a szabály a következő tulajdonsággal kell rendelkezzék: A csoport bármely két eleme – g és h – és ezek csoportbeli gh szorzata esetén az S_{gh} szimetria megegyezik az S_g és S_h szimmetriák kompozíciójával. Azt is megköveteljük, hogy bármely g elem esetén teljesüljön, hogy $S_g(\vec{a} + \vec{b}) = S_g(\vec{a}) + S_g(\vec{b})$ és $S_g(k \cdot \vec{a}) = k \cdot S_g(\vec{a})$ tetszőleges $\vec{a}, \vec{b}$ vektorok és k szám esetén. (Ezeket a szimmetriákat lineáris leképezéseknek nevezzük; lásd a 14. fejezet 2. jegyzetét.)

Egy n-dimenziós tér összes invertálható lineáris transzformációinak csoportját általános lineáris csoportnak nevezik. Azaz az előző bekezdésben szereplő definíció alapján egy adott Γ csoport n-dimenziós reprezentációja ugyanaz, mint Γ-nak $GL(n)$-beli reprezentációja (vagy másképpen egy homomorfizmus Γ-ból $GL(n)$-be, lásd az 1. jegyzetet).

Például, a 10. fejezetben beszéltünk az $SO(3)$ csoport háromdimenziós reprezentációjáról. Az $SO(3)$ csoport minden egyes eleme a gömb egy forgatása, amelyhez hozzárendeljük a gömböt tartalmazó háromdimenziós vektortér megfelelő forgatását (amely maga lineáris transzformáció). Ez $SO(3)$ reprezentációját adja meg a $GL(3)$ csoportban (vagy ekvivalensen egy homomorfizmust $SO(3)$-ból $GL(3)$-ba). Intuitíven a rotációt úgy is felfoghatjuk, mint amely a háromdimenziós vektortéren hat, ezen tér minden egyes vektorát ezen tér egy másik vektorába forgatja. A Langlands-reláció (melyet Langlands-megfeleltetésként is ismernek) egyik oldalán a Galois-csoport n-dimenziós reprezentációját vesszük. A másik oldalon automorf függvényeink vannak, melyeket fel lehet használni arra, hogy az n-dimenziós vektortér szimmetriáinak $GL(n)$ csoportja automorf reprezentációit építsük fel – ámbár nem a valós számok felett, hanem az ún. „adélok" felett. Meg sem kísérelem megmagyarázni, hogy ezek mik, azonban a következő diagram mutatja, hogy a Langlands-reláció mit takar:



Például, a Galois-csoport kétdimenziós reprezentációi összefüggenek az $GL(2)$ csoport automorf reprezentációival, amelyeket a 9. fejezetben elemzett moduláris formákból lehet megszerkeszteni. Ezen reláció általánosítását kapjuk, ha a $GL(n)$ csoportot általánosabb Lie-csoportra cseréljük. Ekkor a reláció jobb oldalán a $GL(n)$ automorf reprezentációja helyett a G csoport automorf reprezentációját kapjuk. A bal oldalon a Galois-csoport reprezentációja lesz az ${}^LG$ Langlands-duális csoportban, nem pedig $GL(n)$-ben (vagy másképpen a Galois-csoportnak a ${}^LG$ csoportba ható homomorfizmusai). További részletekért lásd az összefoglaló cikkemet: Edward Frenkel, *Lectures on the Langlands-program and conformal field theory*, a *Frontiers in Number Theory, Physcis and Geomerty II.* kötetben. Szerk.: P. Cartier, e.a., p. 387–536, Springer-Verlag, 2007. Online elérhetőség:

http://arxiv.org/pdf/hsp-th/0512172.pdf

3. Lásd az alábbi videót:

http://www.youtube.com/eatch?v=CYBqIRM8GiY

4. Ezen tánc neve „binasuan". Lásd pl. az alábbi videót:

http:///www.youtube.com/watch?v=N2T00z_eaTY

5. A görbe megszerkesztésével és azzal kapcsolatosan, hogy ha kétszer megyünk át ezen a görbén, akkor a triviális görbét kapjuk, lásd például Louis H. Kaufmann könyvét: *Knots and Physics*, Theird Edition, p. 419–420., World Scientific, 2001.

6. Más szavakkal, az $SO(3)$ fundamentális csoportja két elemből áll: az egyik az identitás, a másik pedig ez a görbe, melynek a négyzete az identitás.

7. Ezen csoport matematikai neve $SU(2)$. A kétdimenziós komplex vektortér „speciális unitér" transzformációiból áll. Ez a csoport az $SU(3)$ csoport unokatestvére, melyet a 2. fejezetben a kvarkokkal kapcsolatban tárgyaltunk, és amelyik a háromdimenziós komplex vektortér speciális unitér transzformációiból áll.

8. Pontosabban, a most megszerkesztett zárt görbe (amely a bögre első teljes körbefordulásának felel meg) felemelése az $SO(3)$ csoportból a kétszeres fedésébe, az $SU(2)$ csoportba olyan görbe lesz, amely az $SU(2)$ eltérő pontjaiból indul és végződik (mindkettőnek ugyanaz a vetülete az $SO(3)$ csoportban), és így nem lesz zárt görbe $SU(2)$-ben.

9. Általánosságban ez az összefüggés bonyolultabb, azonban az egyszerűség kedvéért ebben a könyvben fel fogjuk tenni, hogy a duális csoport duális csoportja maga az eredeti csoport.

10. Valamely Riemann-felület principális G-nyalábja (röviden G-nyaláb) nem más, mint olyan fibrálás a Riemann-felületen, amelyben minden fibrum a G csoport „komplexifikációjának" (a csoport definíciójában a valós számokat komplex számokra cseréljük) másolata. Az X téren tekintett G-nyalábok modulusterének (pontosabb ezt kupacnak nevezni) pontjai az X-en értelmezett G-nyalábok ekvivalenciaosztályai.

A tárgyalás egyszerűsítése érdekében ebben a könyvben nem teszünk különbséget a Lie-csoport és a komplexifikációja között.

11. A fundamentális csoportban azonosnak tekintjük azokat a zárt görbéket, amelyek folytonos deformációval átalakíthatóak egymásba. Mivel a síkon tetszőleges olyan zárt görbe, amely nem kerüli meg az eltávolított pontot, egyetlen pontra húzható össze, ezért a fundamentális csoport nemtriviális elemei azok a zárt görbék, amelyek körbekerülik ezt a pontot (ezeket nem lehet összehúzni – a síkból eltávolított pont megakadályozza az összehúzást).

Könnyen látható, hogy tetszőleges két zárt görbe, amelyek ugyanazzal a körbejárási számmal rendelkeznek, egymásba átalakítható. Így a síkból

egyetlen pont eltávolításával kapott halmaz fundamentális csoportja nem más, mint az egészek csoportja. Vegyük észre, hogy ez a gondolatmenet emlékeztet az 5. fejezetben, a két fonállal rendelkező fonatok elemzésére, amikor szintén azt kaptuk, hogy megegyezik az egészek csoportjával. Ez nem véletlen egybeesés, mivel a sík két különböző pontjából álló tér topologikusan ekvivalens a síkból egyetlen pont eltávolításával adódó térrel.

12. A híres Euler-képlet,

$$e^{\theta\sqrt{-1}} = \cos(\theta) + \sin(\theta)\sqrt{-1}$$

az oka annak, hogy a monodrómia a kör csoportjából veszi fel értékeit. Más szavakkal, az $e^{\theta\sqrt{-1}}$ komplex szám az egységsugarú kör azon pontjával reprezentálható, amely a θ szögnek felel meg, ha a szöget radiánban mérjük. Emlékezzünk arra, hogy 2π radián egyenlő 360 fokkal. (Ez a kör teljes körbefordulásának felel meg.) Tehát a radiánban mért θ szög értéke $360 \cdot \theta/2\pi$ fok.

Speciális esete ennek a képletnek a $\theta = \pi$ eset, amikor is

$$e^{\pi\sqrt{-1}} = -1\,.$$

Ezt Richard Feynman „az egész matematika egyik legjelentősebb, szinte elképesztő képletének" nevezte. Jelentős szerepet játszott Yoko Ogawa *The Housekeeper and the Professor* című regényében. (Picador, 2009) Egy másik, nem kevésbé fontos speciális eset az $e^{2\pi\sqrt{-1}} = 1$.

Ez azt jelenti, hogy ha a komplex sík pontjainak koordinátáját t jelöli, akkor az egységkör a $t = e^{\theta\sqrt{-1}}$ alakú pontokból áll, ahol θ értéke 0 és 2π között van. A differenciálegyenlet megoldását ezen t függvényében adtuk meg. Ahogy az óramutató járásával ellentétesen mozgunk az egységkörön, az $x(t) = t^n$ megoldást a $t = e^{\theta\sqrt{-1}}$ pontokban számítjuk ki, ahogy a θ szög 0-tól 2π-ig (radiánokban) nő. Teljes kört megtéve θ értéke 2π lesz. Ezért az ehhez tartozó érték meghatározásához be kell helyettesítenünk a $t = e^{2\pi\sqrt{-1}}$ értéket az t^n függvénybe. Az eredmény $e^{2\pi n\sqrt{-1}}$. A megoldás kiinduló értéket úgy kapjuk meg, ha a $t = 1$ értéket helyettesítjük a t^n függvénybe, amelynek értéke 1. Azt kaptuk tehát, hogy amint végigmegyünk az óramutató járásával ellentétesen bejárt egységkörön mint zárt görbén, a megoldásunk értékét a $e^{2\pi n\sqrt{-1}}$ számmal meg kell szorozni. Ez tehát az ezen a görbén adódó monodrómia.

Ez a monodrómia – $e^{2\pi n\sqrt{-1}}$ – olyan komplex szám, melyet egy *másik* komplex sík egységkörének pontjával lehet reprezentálni. Ez a pont a $2\pi n$ radiánnak felel meg, másképpen a $360n$ foknak, és éppen ezt akartuk megmutatni. Valóban, tetszőleges z komplex számot $e^{2\pi n\sqrt{-1}}$ értékkel szorozni

annyit jelent, hogy a z értéknek megfelelő pontot $360n$ fokkal elforgatjuk. Ha n egész szám, akkor $e^{2\pi n\sqrt{-1}} = 1$, azaz nem lép fel a monodrómia, azonban ha n nem egész szám, akkor nemtriviális monodrómiát kapunk.

A félreértés elkerülése érdekében hangsúlyozni akarom, hogy két különböző komplex sík szerepel itt: az egyik az a komplex sík, ahol a megoldást definiáltuk – ez a „t sík". A másik az a sík, ahol a monodrómiát reprezentáljuk. Ennek semmi köze a t síkhoz.

Összefoglalva, a megoldásnak $+1$ körüljárási számmal rendelkező, a t-síkon vett zárt görbe mentén tekintett monodrómiáját egy másik egységkör egy pontja segítségével szemléltettük. Hasonlóképpen, ha a körüljárási szám w, akkor az ezen görbe mentén adódó monodrómia $e^{2\pi wn\sqrt{-1}}$ lesz, amely $2\pi nw$ radiánnal, avagy $360wn$ fokkal való forgatásnak felel meg. Tehát a monodrómia a fundamentális csoportnak az egységkör csoportjában történő reprezentációját eredményezi. Ezen reprezentáció során a kilyukasztott t sík olyan görbéje, melynek w a körüljárási száma, a $360wn$ fokkal történő elforgatásba megy.

13. Vegyük észre, hogy fontos szerepet játszik az origó eltávolítása a síkból. Egyébként minden görbe egy pontba húzható lenne, és így a fundamentális csoport triviális lenne. Ezért ekkor nem lehetséges a monodrómia. Szükség is volt arra, hogy ezt a pontot eltávolítsuk, mert a t^n megoldás nincsen értelmezve az origóban, ha n nem természetes szám vagy 0 (ebben az esetben nincsen monodrómia).

14. Pontosabban, a fundamentális csoport ${}^LG$ -beli reprezentációjának nem mindegyike kapható meg operből. A diagramban azokat adtuk meg, melyekre ez lehetséges. Más reprezentációk esetén a kérdés még nyitott.

15. Edward Frenkel, *Langlands Correspondence for Loop Groups*, Cambridge University Press, 2007. Online elérhetőség:
http://math/berkeley.edu/∼frenkel .

16. fejezet. Kvantumdualitás

1. Az olvasó eltűnődhet azon, hogy vajon mi történt 1991 és 2003 között. Valóban, fő célom ebben a könyvben, hogy a Langlands-program számomra legérdekesebb vonatkozásairól számot adjak, továbbá arról, hogy hogyan születtek ezen a területen a felfedezések, amelyekhez szerencsémre én is hozzájárulhattam. Nem akarok naprakész beszámolót adni az életemről. A kíváncsiak számára mégis elmondom, hogy ezek alatt az évek alatt családomat Oroszországból áthoztam az USA-ba, a nyugati partra, Berkeley-be, Ka-

liforniába költöztem, szerelmes lettem és kiábrándultam, megházasodtam és elváltam, számos PhD hallgatót neveltem fel, utaztam és előadásokat tartottam szerte a világon, könyvet és tucatnyi tudományos cikket írtam. Különböző területeken továbbra is megpróbálom felfedni a Langlands-program rejtélyeit: a geometriától az integrálható rendszerekig, a kvantumcsoportoktól a fizikáig. Utazásom ezen részének részleteit egy másik könyv számára őrzöm meg.

2. Lásd http://www.darpa.mil/Our_Work

3. G. H. Hardy, *A Mathematician's Apology*, Cambridge University Press, 2009, p. 135.

4. Idézet az alábbi szövegből: R. R. Wilson's Congressional Testimony, April 17, 1969.

http://history.fnal.gov/testimony.html

5. Vákuumban a Maxwell-egyenletek a következő alakot öltik:

$$\begin{array}{cc} \nabla \cdot \vec{E} = 0 & \nabla \cdot \vec{B} = 0 \\ \nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t} & \nabla \times \vec{B} = -\frac{\partial \vec{E}}{\partial t} \end{array} ,$$

ahol $\vec{E}$ jelöli az elektromos mezőt és $\vec{B}$ jelöli a mágneses mezőt (a képletek egyszerűbb formája miatt olyan mértékegységrendszert választunk, melyben a fénysebesség pontosan 1). Világos, hogy ha az

$$\vec{E} \to \vec{B}\,, \quad \vec{B} \to \vec{E}$$

cserét megtesszük, akkor a bal oldali egyenletek a jobb oldali egyenletekké alakulnak és megfordítva. Tehát az egyes egyenletek külön megváltoznak, az egyenletrendszer azonban nem.

6. Lásd Dayna Mason „flickr" oldalát:
http://www.flickr.com/photos/daynoir

7. Ezt az $SU(3)$ mércecsoportot nem szabad összekeverni a 2. fejezetben tárgyalt másik $SU(3)$ csoporttal. Ez utóbbit Gell-Mann és mások használták arra, hogy az elemi részecskéket osztályozzák (ezt hívják „ízcsoportnak"). Az $SU(3)$ mércecsoportnak a kvarkok egy másik jellemzőjéhez van köze, ezt „színnek" nevezik. Kiderült, hogy mindegyik kvark három különböző szín egyikével rendelkezik, és az $SU(3)$ mércecsoport a felelős ezen színek cseréjéért. Ezért a kvarkok közötti kölcsönhatásokat leíró mérceelméletet kvantum-színdinamikának nevezik. David Gross, David Politzer és Frank Wilczek kaptak Nobel-díjat azért a meglepő felfedezésért, melyet a kvantum-színdinamikában (és más nem-abeli mérceelméletben) meglévő

aszimptotikus szabadságnak neveznek, és amely segített a kvarkok misztikus viselkedésének értelmezésében.

8. D. Z. Zhang, *C. N. Yang and contemporary mathematics*, Mathematical Intelligencer, vol. 15., No. 4. 1993, p. 13–21.

9. Albert Einstein, *Geometry and Experience*, Address to the Prussian Academy of Sciences in Berlin, January 27, 1921, Fordítás: G. Jeffrey és W. Perrett, *Geometry and Experience in sidelights on Relativity*, Methuen, 1923.

10. Eugene Wigner, *The unreasonable effectiveness in the natural sciences*, Communication on Pure and Applied Mathematics, vol. 13., 1960, p. 1–14.

11. C. Montonen és D. Olive, *Magnetic monopoles as gauge particles*, Physics Letters B, vol. 72., 1997, p. 117–120.

12. P. Goddard, J. Nuyts és D. Olive, *Gauge theories and magnetic charge*, Nuclear Physics B, vol. 125., 1997, p. 1–28.

13. S_e a G maximális tóruszának komplex egydimenziós reprezentációinak halmaza, és S_m a G maximális tóruszának fundamentális csoportja. Ha G a körcsoport, akkor a maximális tórusza saját maga, és ez a két halmaz kölcsönösen egyértelmű megfeleltetésben van az egész számok halmazával.

17. fejezet. Feltárjuk a rejtett kapcsolatokat

1. Az $M(X, G)$ teret többféleképpen lehet leírni; például valamely X-en értelmezett differenciálegyenlet-rendszer megoldásainak halmazaként. (Ezt először Hitchin vizsgálta, további részletekért lásd a lenti 19. jegyzetet). Ebben a fejezetben a későbbiekben számunkra hasznos lesz az a leírás, hogy $M(X, G)$ az S Riemann-felület fundamentális csoportjának a G csoport komplexifikációiba ható reprezentációinak modulustere (lásd a 15. fejezet 10. jegyzetét). Ez azt jelenti, hogy $M(X, G)$ minden egyes pontjához egy ilyenfajta reprezentációt rendelünk.

2. A Hitchin előadásáról szóló videót lásd a Fields Institute honlapján: http://www.fields, utortonto.ca/video-archive/2012/10/108-690

3. Itt Ngô Bao Châu friss kutatásaira utalok, melyet a Langlands-program „fundamentális lemmájának" bizonyításával kapcsolatosan végzett. Lásd pl. a következő áttekintő cikket: David Nadler, *The geometric nature of the fundamental lemma*, Bulletin of the American Mathematical Society, vol. 49., 2012, p.1–50.

4. Ne feledjük, hogy a szigma-modellben mindent úgy számolunk ki, hogy összegzünk a rögzített Σ Riemann-felületnek az S képsokaságba ható összes leképezése szerint. A húrelméletben még egy további lépést teszünk:

azon túlmenően, hogy összegzünk a rögzített Σ-ból az S-be ható leképezések szerint, ahogyan azt a szigma-modellben tesszük, még az összes lehetséges Σ Riemann-felület szerint is összegzünk (az S képsokaság marad végig rögzített – ez a mi téridő-terünk). Speciálisan, tetszőleges génusszal rendelkező Riemann-felületek szerint is összegzünk.

5. A szuperhúrok elméletéről továbbiakat is tartalmaz a következő könyv: Brian Greene, *The Elegant Universe*, Vintage Books, 2003, *The Fabric of the Cosmos: Space, Time and the Texture of Reality*, Vintage Books, 2005.

6. A Calabi–Yau-sokaságokról és a szuperhúrelméletben betöltött szerepükről lásd Shing Tung Yau és Steve Nadis, *The Shape of Inner Space*, Basic Books, 2010, 6. fejezet.

7. A tórusznak két folytonos paramétere van: lényegében az ebben a fejezetben tárgyalt R_1 és R_2 sugarak; a jelen elemzés során azonban ezektől eltekintünk.

8. Az utóbbi időkben aktívan elemzett lehetséges megoldást adna az az ötlet, hogy ezen sokaságok mindegyike saját fizikai törvényekkel rendelkező saját univerzumhoz vezetne, kiegészítve ezt az antropikus elv egy változatával: ezek közül a mi világegyetemünket az a tény választja ki, hogy a fizikai törvényeknek olyanoknak kell lenniük, amelyek lehetővé teszik, hogy létezzen intelligens élet (így tehát megkérdezhető, hogy „miért ilyen a mi világegyetemünk?"). Ugyanakkor ez az elképzelés, szinkronban a „húrelméleti tájképpel" vagy „multiverzummal", számos kritikával szembesült mind tudományos, mind pedig filozófiai alapon.

9. A különböző dimenziójú kvantumtérelméletek számos érdekes tulajdonságát fedezeték fel és értelmezték ezen elméleteknek a szuperhúrelméletekhez való kapcsolásával – a dimenzióredukció, illetve a bránok segítségével. Egy bizonyos értelemben a szuperhúrelméletet mint valamely gyárat használták fel (többnyire szuperszimmetrikus) kvantumtérelméletek gyártására és elemzésére. Például, ezen az úton gyönyörű interpretációját lehet kapni négydimenziós szuperszimmetrikus mérceelmélet elektromágneses dualitásának. Így, bár még nem tudjuk, hogy vajon a szuperhúrelmélet leírja-e a világegyetemünk fizikáját (és még csak nem is értjük teljesen, hogy mi is a szuperhúrelmélet), a kvantumtérelmélettel kapcsolatban máris sok fontos meglátást eredményezett. Továbbá számos területen hozzájárult a matematika fejlődéséhez.

10. Az $M(X, G)$ Hitchin-féle modulustér dimenziója a G csoport dimenziójának (amely megegyezik az ${}^L G$ dimenziójával) és $(g-1)$-nek a szorzata, ahol g jelöli az X Riemann-felület génuszát.

11. A bránokról továbbiakért lásd: Lisa Randall, *Warped Passages: Unraveling the Mysteries of the Universe's Hidden Dimensions*, Harper Perennial, 2006, különösen a IV. fejezet.

12. Pontosabban, az $M(X, G)$ tér A-bránjai egy kategória objektumai. Ezt a fogalmat a 14. fejezetben elemeztük. Az $M(X, {}^L G)$ tér B-bránjai egy másik kategória objektumai. A homologikus tükörszimmetria állítása az, hogy ez a két kategória ekvivalens egymással.

13. Anton Kapustin and Edward Witten, *Electric-magnetic duality and the geometric Langlands-program*, Communication in Number Theory and Physics, vol. 1., 2007, p. 1–236.

14. A T-dualitásról továbbiakért lásd a 6. jegyzetben idézett Yau és Nadis könyv 7. fejezetét.

15. Az SYZ-sejtésről továbbiakért lásd a 6. jegyzetben idézett Yau és Nadis könyv 7. fejezetét.

16. Pontosabban mindegyik fibrum n kör szorzata, ahol n páros természetes szám, így tehát ez a kétdimenziós tórusz n-dimenziós megfelelője. Jegyezzük meg, hogy a Hitchin-fibrálás alapterének dimenziója és a tóruszfibrumok dimenziói mindig megegyeznek egymással.

17. A 15. fejezetben ettől eltérő konstrukciót elemeztünk. Ebben az automorf kévéket a Kac–Moody-algebrák reprezentációiból kaptuk. Várható, hogy a két konstrukció összefügg, azonban a jelen könyv megírásának időpontjáig ez még nem bizonyított.

18. Edward Frenkel and Edward Witten, *Geometric endoscopy and mirror symmetry*, Communications in Number Theory and Physics, vol. 2., 2008, p. 113–283. Online elérhetőség:
http://arxiv.org/pdf/0710.5939.pdf

19. Edward Frenkel, *Gauge theory and Langlands duality*, Astérisque, vol. 332., 2010, p. 369–403. Online elérhetőség:
http://arxiv.org/pdf/0906.2747.pdf

20. Henry David Thoreau, *A Week in the Concord and Merrimack Rivers*, Penguin Classics, 1998, p. 291.

18. fejezet. Keressük a szerelem rejtett képletét

1. C. P. Snow, *The Two Cultures*, Cambridge University Press, 1998.

2. Thomas Farber and Edward Frenkel, *The Two-Body Problem*, Andrea Youn Arts, 2012. További részletekért lásd:
http://thetwobodyproblem.com/

3. Michael Harris, *Further investigation of the mind-body problem*, fejezet egy készülő könyvből. Online elérhetőség:
http://wwww.math.jussieu.fr/∼ harris/ MindBody.pdf

4. Henry David Thoreau, *A Week on the Concord and Merrimack Rivers*, Penguin Classics, 1998, p. 291.

5. E. T. Bell, *Men of Mathematics*, Touchstone, 1986, p. 16.

6. Robert Langlands, *Is there beauty in mathematical theories?*, Lásd: *The Many Faces of Beauty*, szerk. Vittorio Hösle, University of Notre Dame Press, 2013. Online elérhetőség:
http://publications.ias.edu/sites/default/files/ND.pdf

7. Yuri I. Manin, *Mathematics as Metaphor: Selected Essays*, American Mathematical Society, 2007, p. 4.

8. A filozófusok évszázadokon keresztül megkérdőjelezték a matematika lételméletét. Azt az álláspontot, melyet ebben a könyvben képviselek, rendszerint matematikai platonizmusnak nevezik. Jegyezzük meg ugyanakkor, hogy a platonizmusnak különböző változatai vannak, emellett a matematikának más filozófiai interpretációi is vannak. Lásd például Mark Balagues, *Mathematical Platonism*, szerk. Bonnie Gold és Roger Simons *Proof and Other Dilemmas: Mathematics and Philosophy*, Mathematics Association of America, p. 179–204, és az ottani hivatkozások.

9. Roger Penrose, *The Road to Reality*, Vintage Books, 2004, p. 15.

10. Ibid. pp. 13–14.

11. Kurt Gödel, *Collected Works*, Volume III, Oxford University Press, 1995, p. 320.

12. Ibid, p. 323.

13. Roger Penrose, *Shadows of the Mind*, Oxford University Press, 1994, Section 8.4.7.

14. A határkövet jelentő *Gottschalk v. Benson* döntésben, 409 U.S. 63(1972) az USA Legfelsőbb Bírósága kijelentette (korábbi bírósági eseteket idézve): „tudományos igazság vagy annak matematikai kifejezése nem szabadalmazható felfedezés... Egy elv, absztraktan egy alapvető igazság, egy eredeti ok, egy indítóok; ezeket nem lehet szabadalmaztatni, és senki sem jelentheti ki, hogy ezek felett kizárólagos joga van... Az, aki felfedez egy eddig még nem ismert természeti jelenséget, nem rendelkezik azzal a joggal, hogy a törvény által elismerten kisajátítsa azt.

15. Edward Frenkel, Andrey Losev and Nikita Nekrasov, *Instantons beyond topolical theory I*, Journal of the Institute of Jussieu, vol. 10., 2011, p. 463–565. Itt szerepel egy lábjegyzet, amely megmagyarázza, hogy az

(5.7) képlet miért játszotta a „szerelem képletének" szerepét a *Rites of Love and Math* c. filmben.

16. Tekintsük a gömbön (amit $\mathbb{CP}^1$ jelöl) a szuperszimmetrikus kvantummechanikai modellt és két megfigyelés – F és ω – közötti korrelációs függvényt. Elméletünkben ezt a korrelációs függvényt a képlet bal oldalán szereplő kifejezés definiálja. Ugyanakkor az elméletünk szerint egy másik kifejezés is van erre: a jobb oldalon lévő „közbülső állapotok" szerinti összeg. Elméletünk ellentmondásmentessége megköveteli, hogy a két oldal egyenlő legyen egymással. És valóban azok is: ez az, amit a képletünk megfogalmaz.

17. *Le Monde Magazine*, April 10, 2010, p. 64.

18. Laura Spinney, *Erotic equations: Love meets mathematics on film*, New Scientist, April 2010, p. 6-8. Online elérhetőség:
http://ritesofloveandmath.com

19. Hervé Lehning, *La dualité l'amour et les maths*, Tangente Sup. vol. 56., May-June 2010, p. 6–8. Online elérhetőség: http://ritesofloveandmath.com

20. Anna Akhmatova, a 20. század első felének nagy orosz költőnője költeményét használtuk fel, melynek címe: *To the Many*.

21. Norma Farber, *A Desperate Thing*, The Plowshare Press Incorporated, 1973, p. 21.

22. Einstein levele Pyllis Wrighthoz. 1936. január 24. Idézi Walter Isaacson az *Einstein: His Life and Universe* című könyvében. Simon & Schuster, 2007, p. 388.

23. David Brewster, *Memoirs of the Life, Writings, and Discoveries of Sir Isaac Newton*, vol. 2. Adamant Media Corporation, 2001 (az 1855-ös kiadás – Thomas Constable and Co. – újranyomása), p. 407.

Epilógus

1. Edward Frenkel, Robert Langlands és Ngô Bao Châu, *Formule des Traces et Fonctorialité: le Début d'un Programme*, Annales des Sciences Mathématiques de Québecv vol. 4., 2010, p. 199–243. Online elérhetőség:
http://arxiv.org/pdf/1003.4578.pdf

Edward Frenkel, *Langlands Program, trace formulas, and their geometrization*, Bulletin of AMS, vol. 50 (2013) 1–65. Online elérhetőség:
http://arxiv.org/pdf/1202.2110.pdf