Bevezetés az absztrakt algebrába

Hermann Péter és Kiss Emil

Tartalom

Bevezetés a jegyzethez

Te jól tudod, a költő sose lódít:
az igazat mondd, ne csak a valódit.

József Attila: *Thomas Mann üdvözlése*

Ez a jegyzet egy most készülő könyv kézirata. Bármilyen megjegyzést, javítást, kérést szívesen veszünk, sőt reméljük, hogy minél több ilyen megjegyzést kapunk, mert ez javítani fogja a könyv színvonalát. A megjegyzéseket az `ewkiss@cs.elte.hu` email-címre érdemes küldeni, de szívesen meghallgatjuk szóban is. A visszajelzések birtokában a jegyzetet folyamatosan javítjuk, és ahogy az előadás halad előre, újabb anyagrészekkel bővítjük is. Ezért érdemes rendszeresen körülnézni a

`http://www.cs.elte.hu/~ewkiss/bboard/algebrabook/`

web-címen, ahol `pdf` formátumban mindig megtalálható a legfrissebb változat, és az ismert, értelemzavaró sajtóhibák jegyzéke is.

A könyv matematika tanárszakos, matematikus, és alkalmazott matematikus hallgatók számára készül. E három szakon az anyag mennyisége, felépítése, és így az előadás tempója, részletessége is különböző lehet. Sok esetben az előadó egyes számolásokat, meggondolnivalókat házi feladatnak ad azért, mert ezeket önálló munkával lehet csak igazán megérteni. A jegyzet azzal kínál segítséget, hogy benne vannak azok a részletek is, amelyek az előadáson nem mindig hangzanak el. Ezek sokszor magyarázatok, részletszámítások, de elsősorban az apróbetűs részekben szerepelnek mélyebb, előremutató, vagy filozófiai jellegű megjegyzések is.

Maximális érthetőségre törekedtünk, de ezen belül mindig úgy választottuk a tárgyalási módot, hogy a lehető legjobban előkészítse a legfontosabb absztrakt algebrai fogalmak bevezetését. Ezért a bevezető fejezeteket annak is érdemes átfutnia, aki már ismeri például a komplex számokat, vagy a polinomokat. Nagy hangsúlyt fektettünk arra, hogy elmagyarázzuk a „miért”-eket: azt, hogy az egyes fogalmak miért fontosak, miért így és nem máshogy definiáltuk őket, hogy a bizonyításokban miért éppen a leírt lépéseket tesszük, hogy lehetne-e másmerre haladni. Úgy gondoljuk, ez nemcsak az anyag alkalmazásához ad segítséget, hanem az önálló problémamegoldáshoz is. Aki a matematikát alkalmazza, azaz modelleket készít, annak el kell sajátítania a fogalomalkotás technikáját is.

A jegyzet formája annyiban szokatlan, hogy egyes számolási részletek, meggondolnivalók Kérdés, Gyakorlat, vagy akár Feladat formájában szerepelnek az „elméleti” szövegen

belül is. Meggyőződésünk, hogy matematikát úgy lehet a legeredményesebben tanulni, ha minél több bizonyítást magunk találunk ki, és ha menet közben elgondolkozunk a dolgokon, mielőtt tovább olvasnánk. Az új forma ennek a lehetőségét próbálja megteremteni. Ha valaki nem boldogul egy ilyen Kérdés megválaszolásával, vagy ha ellenőrizni akarja magát, akkor érdemes a választ fellapoznia a jegyzet végén, mielőtt tovább haladna.

A matematikát nem elég megtanulni, meg is kell érteni azt. Ebben segítenek a könyvben szereplő Gyakorlatok (ezek általában könnyebbek), és a Feladatok (amelyek nehezebbek). Ezek legtöbbjéhez megoldást, és a Feladatokhoz ezen kívül útmutatást is adunk a jegyzet végén. Így a jegyzetben csaknem teljes egészében megtalálható a gyakorlatokon szerepelt anyag is, megoldásokkal együtt.

Vigyázzunk: a megoldások elolvasása nem helyettesíti az önálló gondolkodást. Ezen kívül a megértés és a begyakorlás két különböző dolog! A jegyzetben szereplő Gyakorlatok és Feladatok elsősorban az anyag megértését segítik. Ha nem elegendőek a begyakorlásra, akkor a Fagyejev-Szominszkij [**2**] és a Czédli-Szendrei-Szendrei [**1**] feladatgyűjteményekből érdemes további feladatokat megoldani, egyéni szükségletek szerint.

A jegyzet kiindulásképpen csak a középiskolai anyagra támaszkodik. Ahogy azonban haladunk előre, szükség lesz más, elsősorban számelméleti, kombinatorikai, és később lineáris algebrai ismeretekre is. Ezek elsajátításában segíthetnek az Irodalomjegyzékben szereplő művek, elsősorban Freud Róbert és Gyarmati Edit: *Számelmélet* [**4**], illetve Freud Róbert: *Lineáris algebra* [**3**] című művei. A szövegben természetesen mindig megemlítjük a szükséges előismereteket.

Végül egy általános megjegyzést szeretnénk tenni a matematikáról. A matematika fejlődése nem olyan egyszerű folyamat, hogy megoldjuk a gyakorlatban, vagy a más tudományokban felmerülő problémákat. Azért nem, mert sokszor előfordul, hogy ezeket a problémákat nem tudjuk megoldani azonnal. Gyakori tapasztalat, hogy ilyenkor segíthet a megoldásban a matematika egy másik területe, egy olyan terület, amelyet eredetileg egészen más célból, más problémák megoldása végett fejlesztettek ki. Példaként érdemes megemlíteni az RSA titkosítási rendszert, amelyet manapság állandóan alkalmaznak, és amely annak köszönheti a megszületését, hogy az emberiség egy másik, teljesen elvontnak és alkalmazhatatlannak tűnő problémát vizsgált: azt, hogy nagyon nagy számokat milyen eljárással lehet gyorsan prímtényezőkre bontani.

A matematikát tehát nem egy (tétel)gyárhoz érdemes hasonlítani, hanem inkább a természethez, ahol minden mindennel összefügg. Egy-egy terület életképességét az szabja meg, hogy hogyan tud beleilleszkedni az egészbe, milyen kapcsolatokat tud teremteni. A fejlődést sokszor belső törvényszerűségek szabályozzák, ilyen például a matematika esztétikuma. A matematikusok által izgalmasnak, érdekesnek, szépnek tartott kérdések megválaszolása számtalanszor vezetett döntő áttöréshez. Olyan ötletek merülhetnek így fel, amelyhez máshogy el sem juthattunk volna. A matematikát alkalmazni szándékozók azután meglátogathatják a természetet, és megtalálhatják azt az erdei gyümölcsöt, gombát, amire éppen szükségük van.

Ha kirándulunk a természetben, akkor meg is erősödünk. A matematikával való foglalkozás pedig megerősíti az általános emberi gondolkodásnak egy nagyon fontos fajtáját: azt, amikor szisztematikusan végig kell gondolnunk valamit. Ez lehet köznapi dolog, mondjuk bútortologatási stratégia egy zsúfolt lakásban, de lehet számítástechnikai probléma, vagy akár jogi kérdés is. Mindezt problémamegoldással, fogalmak, bizonyítások megértésével edzhetjük. A matematikának része a matematikai logika, amely ezt a fajta gondolkodásmódot vizsgálja, és teljes megbízhatósággal kezeli.

Minden kedves olvasónak hasznos, sikeres időtöltést, és kellemes, élményekben gazdag kirándulást kívánunk.

Budapest, 2003 őszén:

Hermann Péter és Kiss Emil

I. rész

Elemi algebra

1. KOMPLEX SZÁMOK

... a zseniális Cerebron, egzakt módszerekkel boncolgatva a problémát, a sárkányok három faját fedezte fel: a nullás, az imaginárius, és a negatív sárkányokat. Mindezek, amint már említettük, nem léteznek, de mindegyik fajta egészen másképpen nem létezik.

Stanisław Lem: *Kiberiáda*
(Murányi Beatrix fordítása)

1.1. Műveletek és tulajdonságaik

Mit is jelent az, hogy „kiszámolunk" valamit? A mindennapi életben mondhatjuk ezt olyankor is, ha el akarjuk dönteni, melyik úton haladva jutunk el leggyorsabban a Magas-Tátrába, vagy hogy beáldozzuk-e a vezérünket egy sakkpartiban a gyorsabb mattadás érdekében. Amikor matematikáról van szó, akkor elsősorban arra gondolunk, hogy *műveleteket végzünk:* összeadunk, kivonunk, szorzunk, osztunk.

Ha megkérdeznénk valakit, hogy *miket* szoktunk így összeadni vagy kivonni, akkor valószínűleg azt a választ kapnánk, hogy számokat. De milyen számokat? Egy ősember valószínűleg kis pozitív egész számokra gondolna: egy, kettő, három, sok. A régi görögök csak a racionális számokat tekintették számnak. A törteket ismerték, de a végtelen tizedes törteket nem. A szakaszok hosszát csak geometriailag tudták összeadni, és még be is bizonyították, hogy az egységnégyzet átlója *nem szám*, hiszen nem lehet két egész hányadosaként kifejezni. Ha pedig egy modern fizikussal találkozunk, akkor ő függvényekről, mátrixokról, kvaterniókról, lineáris operátorokról, és még ki tudja mi mindenről fog beszélni, amiket ő mind-mind össze szeretne adni.

A matematika dolga ebben a helyzetben az lenne, hogy ezeknek az embereknek megkönnyítse a számolások elvégzését. De nem mindegy, hogy hogyan! Ha valakinek sok olyan feladatot kell megoldania, ami mind másodfokú egyenletre vezet, akkor minden egyenlettel szaladjon a matematikushoz? Jobban jár, ha a matematikus ehelyett megmutatja neki a megoldóképletet. A matematika erős oldala mindig is az volt, hogy sok hasonló problémát *egyszerre* tudott megoldani, alkalmas módszerek kidolgozásával.

A fenti helyzetben, amikor sok ember mindenfélével számolni akar, az a jó, ha a matematikus egyszerre tud segíteni nekik, olyan általánosan, ahogy csak lehet. Arra kell

koncentrálnia, hogy mik a *műveletek közös tulajdonságai*, amiket azután a kliensei (vagy kliensek nagyobb csoportjai) használni tudnak. Az absztrakt algebra elsősorban az ilyen tulajdonságokkal foglalkozik.

Ahhoz, hogy mindezt megértsük, konkrét példákat kell látnunk. Kezdetnek három ilyen példa kínálkozik. Amikor egyenleteket oldunk meg, akkor már nem számokkal számolunk, hanem olyan kifejezésekkel, amikben ismeretlenek is szerepelnek. Ez fog bennünket elvezetni a *polinomok* fogalmához. A magasabb fokú egyenletek megoldásakor, és számos más alkalmazásban is, az úgynevezett *komplex számok* lesznek hasznosak. Számelméleti és kombinatorikai feladatok megoldásakor néha érdemes a számoknak csak a paritását, vagy valamilyen számmal vett osztási maradékát vizsgálni. Ilyenkor *maradékokkal* számolunk. Meg fogjuk látni, hogy a számolás szabályai mindhárom esetben hasonlóak lesznek.

A fejezet hátralévő részében a maradékokkal való számolás hasznosságát próbáljuk meg illusztrálni néhány feladattal. Az alábbi két feladat nagyon különböző, de a megoldásuk ötlete hasonló.

1.1.1. Feladat. Igazoljuk, hogy egy 100×100-as sakktábla nem fedhető le 8×1-es dominókkal (egyrétűen és hézagmentesen).

1.1.2. Feladat. Megoldható-e az egész számok körében az $x^2 + 5y = 1002$ egyenlet?

Az első feladat megoldásához írjunk fel a sakktábla minden mezőjére egy-egy számot a következőképpen. A bal felső sarokba nullát írunk. Ezután a sor többi elemét úgy töltjük ki, hogy az előző mezőn lévő számhoz mindig 1-et hozzáadunk, de ha a 8-hoz érünk, akkor nem 8-at, hanem nullát írunk ismét. Ezt úgy fejezzük ki, hogy az 1 hozzáadását *modulo* 8 *végezzük el.* Ha már az első sor kész, akkor ebből kiindulva az összes oszlopot is hasonlóan készítjük el: lefelé haladva minden mező értékét megnöveljük 1-gyel modulo 8. Másképp fogalmazva: a (felülről számított) i-edik sor j-edik mezőjére írt szám az $i + j - 2$ maradéka 8-cal osztva. A bal felső sarok tehát így néz ki:

0	1	2	3	4	5	6	7	0	1
1	2	3	4	5	6	7	0	1	2
2	3	4	5	6	7	0	1	2	3
3	4	5	6	7	0	1	2	3	4
4	5	6	7	0	1	2	3	4	5
5	6	7	0	1	2	3	4	5	6
6	7	0	1	2	3	4	5	6	7
7	0	1	2	3	4	5	6	7	0
0	1	2	3	4	5	6	7	0	1
1	2	3	4	5	6	7	0	1	2

Könnyen látható, hogy *bármely* mezőről egyet jobbra vagy lefelé lépve a ráírt érték pontosan 1-gyel növekszik modulo 8. Helyezzünk most rá egy 8×1-es dominót erre a sakktáblára, akár vízszintesen, akár függőlegesen. Bármilyen számot takar is el a dominó bal felső sarka, a következő eltakart szám ennél eggyel nagyobb modulo 8, a következő még eggyel,

és így tovább. Mivel a dominó nyolc négyzetből áll, mindenképpen a 0, 1, 2, 3, 4, 5, 6, 7 számokat takarja el, valamilyen sorrendben.

Most már könnyű belátni, hogy a kívánt lefedés nem lehetséges. Ha ugyanis létezne ilyen lefedés, akkor, mivel mindegyik dominó pontosan egy darab 0-t takar el, a sakktáblán annyi 0 szerepelne, mint amennyi a szükséges dominók száma. Ugyanennyi szerepelne az 1, 2, 3, 4, 5, 6, 7 számok mindegyikéből is. De ez nem így van, könnyű megszámolni, hogy a sakktáblára 1249 darab 0-t, de csak 1248 darab 7-est írtunk.

1.1.3. Gyakorlat. Mutassuk meg, hogy a sakktáblára több nullát írtunk, mint hetest, *anélkül, hogy megszámolnánk, melyikből hányat írtunk.*

A most alkalmazott gondolatmenet egy *indirekt bizonyítás* volt: feltételeztük, hogy a bizonyítandó állítás hamis (azaz, hogy létezik lefedés), és ebből *ellentmondásra* jutottunk (hiszen az jött ki, hogy $1248 = 1249$). Ezért a kiinduló állításunk sem lehetett hamis, tehát mégsincs ilyen lefedés. Ezt a bizonyítási módot lépten-nyomon alkalmazni fogjuk.

Az 1.1.2. Feladat megoldásához „modulo 5” fogunk számolni. A jobboldalon álló 1002 szám maradéka 5-tel osztva 2. Mivel $5y$ maradéka nulla, olyan x-et kell találnunk, melyre x^2 maradéka szintén 2. Meg fogjuk mutatni, hogy nincs ilyen x, tehát az egyenletnek nincs megoldása az egész számok között.

Ehhez elvileg végig kellene néznünk az összes egész számot, mindegyiket négyzetre emelni, és öttel elosztani. A nullától indulva a keletkező maradékok a következők lesznek:

0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	...
0,	1,	4,	4,	1,	0,	1,	4,	4,	1,	0,	1,	4,	4,	1,	...

Láthatjuk, hogy a sorozat 5-ösével periodikus. Így van-e ez akkor is, ha tovább folytatjuk a sorozatot, vagy ha a negatív x-eket is megvizsgáljuk? A válasz igenlő. Ennek belátásához az x számot osszuk el maradékosan 5-tel: $x = 5q + r$, ahol r a 0, 1, 2, 3, 4 valamelyike. Ekkor

$$x^2 = (5q + r)^2 = 25q^2 + 10q + r^2 = 5(5q^2 + 2q) + r^2 .$$

Vagyis az x^2 és az r^2 ugyanazt a számot adja maradékul! Ezért elég az r^2 lehetséges maradékait végignézni. Ezt már megtettük, és látjuk, hogy a 2 nem fordul elő közöttük, tehát a feladatot megoldottuk: az egyenletnek nincs egész megoldása.

Az előző feladatban az eredeti szám, azaz x helyett annak az 5-tel való osztási maradékával számoltunk. Ez óriási könnyebbség volt, mert végtelen sok szám helyett csak véges sokat — az öt lehetséges maradékot — kellett megvizsgálni. A megoldást az tette lehetővé, hogy szoros kapcsolat volt x^2 és r^2 maradéka között. Hasonló állítás igaz általában az összeadásra és a szorzásra is, durván fogalmazva összeg maradéka a maradékok összege, szorzat maradéka a maradékok szorzata lesz. Emiatt tetszőleges olyan egyenletet, amelyben az ismeretlenek egész számok, megpróbálhatunk úgy megvizsgálni, hogy „modulo 5 vesszük”, vagyis az ismeretlenek helyett azok 5-tel való osztási maradékával számolunk. Ha így nincs megoldás, akkor eredetileg sem lehetett. Persze az 5 helyett más „modulust” is kereshetünk, ha az egyenlet vizsgálatához az a célszerűbb.

Hogyan is végezzük ezeket a műveleteket a maradékok között? Foglaljuk össze táblázatosan az összeadást is és a szorzást is. Az a elemhez tartozó sor és a b elemhez tartozó oszlop metszéspontjában az a és b modulo 5 vett összege illetve szorzata szerepel:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ezekből a táblázatokból sok hasznos információ olvasható le. Például a szorzástábla „főátlójára” nézve látjuk azt a korábban már felhasznált tényt, hogy modulo 5 a 0, 1, 4 számoknak van „négyzetgyöke”, 2-nek és 3-nak pedig nincs. Máshogy fogalmazva: egy négyzetszám 5-tel osztva nem adhat sem 2-t, sem 3-at maradékul.

A fenti táblázatokkal két *új műveletet* definiáltunk a $\{0, 1, 2, 3, 4\}$ halmazon, vagyis a modulo 5 maradékok halmazán. E műveletek tulajdonságai nagyon hasonlítanak az eredeti összeadás és szorzás tulajdonságaihoz. Foglaljuk össze ezeket a tulajdonságokat, de most már általában, az 5 helyett tetszőleges m modulust alkalmazva.

1.1.1. Definíció. Legyen m pozitív egész szám, és jelölje $\mathbb{Z}_m$ a $\{0, 1, \dots, m-1\}$ halmazt, vagyis a modulo m maradékok halmazát. Értelmezzük e számok között a *modulo m összeadást és szorzást* a következőképpen. Ha $a, b \in \mathbb{Z}_m$, akkor $a +_m b$ jelölje az (egész számok között kiszámított) $a + b$ összeg m-mel való osztási maradékát. Hasonlóképpen legyen $a *_m b$ az ab szorzat m-mel való osztási maradéka.

1.1.2. Állítás. *Legyen $m \geq 1$ egész és $x, y, z \in \mathbb{Z}_m$. A jobb áttekinthetőség kedvéért jelölje $+ = +_m$ a modulo m összeadást, $* = *_m$ pedig a modulo m szorzást.*

(1) $(x + y) + z = x + (y + z)$ *(az összeadás* ***asszociatív****).*
(2) $x + y = y + x$ *(az összeadás* ***kommutatív****).*
(3) $x + 0 = 0 + x = x$ *(azaz létezik* ***nullelem****, amelyet bármely elemhez hozzáadva azt az elemet kapjuk).*
(4) *Minden x-nek van* ***ellentettje****, azaz olyan y, melyre $x + y = y + x = 0$. (Ilyen y lesz a $-x$ maradéka modulo m.)*
(5) $(x * y) * z = x * (y * z)$ *(a szorzás asszociatív).*
(6) $x * y = y * x$ *(a szorzás kommutatív).*
(7) $x * 1 = 1 * x = x$ *(azaz létezik* ***egységelem****, amellyel bármely elemet megszorozva azt az elemet kapjuk).*
(8) $(x + y) * z = x * z + y * z$ (***disztributivitás****).*

Ezeket a tulajdonságokat most nem bizonyítjuk be (bár némelyiket könnyű ellenőrizni). A legtöbbjük következik az alábbi állításból, ami a modulo m műveletek és az egész számok közötti műveletek már emlegetett kapcsolatát írja le. Az állítás megfogalmazásához

egy x egész szám m-mel való osztási maradékát egyszerűen csak felülvonással, vagyis $\overline{x}$-sal jelöljük. Ezt persze csak akkor tehetjük meg, ha már előre megbeszéltük, hogy mi az m modulus!

1.1.3. Állítás. *Ha $m \geq 1$ egész, $x, y \in \mathbb{Z}$, és felülvonás jelöli a modulo m maradék képzését, akkor*

$$\overline{x+y} = \overline{x} +_m \overline{y} \quad \text{és} \quad \overline{xy} = \overline{x} *_m \overline{y}\,.$$

Máshogy fogalmazva: összeg maradéka a maradékok (modulo m vett) összege, és szorzat maradéka a maradékok (modulo m vett) szorzata. Röviden: a modulo m maradékképzés összeg- és szorzattartó, azaz ***műveletтartó.***

Nem beszéltünk a kivonás és az osztás műveletéről. Elvégezhetjük-e ezeket is modulo m? A *kivonást* az összeadásból származtatjuk, hiszen $z = x - y$ az a szám, amelyre $z + y = x$. Szerencsére ezzel a művelettel nem kell külön foglalkoznunk, mert visszavezethető az ellentettképzésre. Valóban, az egész számok között $x - y$ megkapható úgy, mint $x + (-y)$ (szavakban: az y kivonása az y ellentettjének a hozzáadása). Ugyanez a helyzet akkor is, amikor modulo m számolunk.

1.1.4. Feladat. Igazoljuk az 1.1.3 és az 1.1.2 állításokat. Definiáljuk alkalmasan a kivonás $-_m$ műveletét, és mutassuk meg az $\overline{x-y} = \overline{x} -_m \overline{y}$ azonosságot.

Az *osztás* művelete ugyanúgy származik a szorzásból, mint ahogy a kivonás az összeadásból: $z = x : y$ az a szám, amelyre $z * y = x$. Ahogy a kivonás az ellentett képzésére, az osztás a *reciprok* (más néven *inverz*) képzésére vezethető vissza. Az y reciproka (vagy inverze) az az $u = 1/y$-nal (néha y^{-1}-gyel) jelölt szám, melyre $y * u = u * y = 1$ (az egységelem). Ha ezt ismerjük, akkor $x : y$ megkapható úgy, mint $x * u$ (szavakban: az y-nal való osztás a reciprokával való szorzás).

A reciprokképzés (és így az osztás) azonban nem végezhető el korlátlanul. Például a nullának egész biztosan nincs reciproka, hiszen $u * 0 = 0$ minden u-ra, és így soha nem kapunk 1-et. Az egész számok között csak az 1-nek és a -1-nek van olyan reciproka, ami szintén egész szám, tehát csak ezekkel lehet korlátlanul osztani. Mint az alábbi gyakorlat illusztrálja, modulo m számolva a helyzet ennél jobb egy kicsit.

1.1.5. Gyakorlat. Végezzük el a fenti modulo 5 szorzástábla alapján a $2 : 3$ osztást modulo 5. Tudunk-e osztani $\mathbb{Z}_5$ minden nem nulla elemével? Mi a helyzet modulo 6?

Az eddigiek alapján leszűrhetjük, hogy modulo m maradékokkal ugyanúgy a „szokásos szabályok” szerint számolhatunk, mint valós számokkal, bár az osztásnál óvatosnak kell lennünk. A következő gyakorlat további óvatosságra int.

1.1.6. Gyakorlat. Igaz-e modulo 5 illetve modulo 6, hogy szorzat csak akkor lehet nulla, ha valamelyik tényezője nulla? (Ezt a tulajdonságot ***nullosztómentesség***nek hívjuk.)

A tanulság, hogy meg kell majd vizsgálnunk pontosan, mit is értünk a „szokásos” számolási szabályokon: fel kell sorolnunk, hogy mit és hogyan szabad csinálnunk, amikor

a műveleteket végezzük. Mielőtt ezt megtennénk, megismerkedünk két másik „struktúrával”, melyekben szintén a „szokásos” szabályok alapján lehet az összeadást és a szorzást elvégezni.

Aki már hallott *maradékosztályokról* számelméletből, az bizonyára ismerősnek találja a fentieket. Ha például modulo 5 nem maradékokkal, hanem maradékosztályokkal akarunk számolni, akkor nem a 2 maradékot tekintjük, hanem helyette a 2 maradékosztályát, vagyis az $5k+2$ alakú számok halmazát. Bár ez matematikailag elegánsabb megközelítés, a műveletek definíciója ilyenkor kissé bonyolultabb lesz, mint az imént. A fellépő nehézségekről részletesen szólunk majd, amikor faktorgyűrűkről beszélünk az 5.2. Szakaszban. Az alkalmazások tekintetében a két módszer egyenértékű.

Gyakorlatok, feladatok

1.1.7. Gyakorlat. Melyek helyesek az alábbi gondolatmenetek közül?

(1) Belátjuk, hogy az $x^2 + 10y^2 = 6$ egyenletnek van megoldása az egész számok körében. Tekintsük az egyenletet modulo 5. Ekkor azt kapjuk, hogy $\overline{x} *_5 \overline{x} = 1$. Ennek van megoldása, például az $x = 1$. Tehát az eredeti egyenlet is megoldható.
(2) Ugyanez a gondolatmenet az $x^2 + 5y^2 = 6$ egyenlet esetén.

1.1.8. Gyakorlat. A modulo 5 műveleti táblázatok vizsgálatával igazoljuk, hogy $a^5 - a$ minden egész a-ra osztható 5-tel. Milyen a egészekre igaz, hogy $a^4 - 1$ osztható 5-tel?

1.1.9. Gyakorlat. Készítsük el a modulo 6 maradékok összeadás és szorzástábláját. Milyen a egészekre teljesülnek az alábbi oszthatóságok?

(1) $6 \mid a^6 - a$.
(2) $6 \mid a^5 - 1$.
(3) $6 \mid a^2 - 1$.

1.1.10. Gyakorlat. Bizonyítsuk be a modulo 8 szorzás felhasználásával, hogy minden páratlan szám négyzete 8-cal osztva 1-et ad maradékul. Mutassuk meg ezt az állítást közvetlen számolással is.

1.1.11. Gyakorlat. Adjunk meg a modulo 5 szorzástábla vizsgálatával olyan x és y egészeket, melyre $5x + 3y = 7$. Véges, vagy végtelen sok megoldás van?

1.1.12. Gyakorlat. Mely x egész számokra teljesül, hogy $5 \mid x^2 - 2x + 2$? És az, hogy $7 \mid x^2 - 2x + 2$?

1.1.13. Feladat. Mely x egészekre teljesül, hogy

(1) $101 \mid x^2 - 2x + 2$?
(2) $101 \mid x^2 - 13x - 3$?

1.1.14. Gyakorlat. A közönséges 8×8-as sakktáblából kivesszük az egyik átló két végpontján lévő két sarokkockát. Lefedhető-e a kapott alakzat 2×1-es dominókkal?

1.1.15. Feladat. Igazoljuk, hogy egy $k \times k$ méretű sakktábla akkor és csak akkor fedhető le $m \times 1$-es dominókkal, ha m osztója k-nak.

1.1.16. Feladat. Igazoljuk, hogy ha p is és p^2+2 is prímszám, akkor p^3+4 is az. Igaz-e, hogy ha p is és p^2+5 is prímszám, akkor p^3+4 is az?

1.2. A harmadfokú egyenlet megoldásának problémája

Ebben a fejezetben a harmadfokú egyenlet vizsgálata kapcsán bemutatjuk, hogy a valós számokat érdemes kibővíteni a megoldások meghatározása érdekében. Ehhez először gondoljuk végig, hogyan is oldjuk meg a másodfokú egyenletet. A megoldóképlet az egyenlet megoldását négyzetgyökvonásra vezeti vissza.

1.2.1. Kérdés. Az $x^2+px+q=0$ egyenletben vezessük be az $y=x-w$ ismeretlent. Hogyan válasszuk meg w értékét, ha azt akarjuk, hogy y értékét egy négyzetgyökvonással közvetlenül megkaphassuk?

A másodfokú egyenlet megoldásakor alkalmazott (az előző kérdésre adott válaszból adódó) $x \mapsto x - p/2$ helyettesítés azért működik, mert általa kiesik az x-es tag, és mivel a $w=-p/2$ kifejezhető az eredeti egyenlet együtthatóiból, az átalakított egyenlet megoldásaiból az eredeti egyenlet megoldásait is megkaphattuk.

Próbáljuk most megoldani az

$$ax^3+bx^2+cx+d=0 \qquad (a\neq 0) \tag{1.2.1}$$

harmadfokú egyenletet. Most is megpróbálkozhatunk azzal, hogy az $x \to x+w$ helyettesítéssel hozzuk az egyenletet egyszerűbb alakra. Ahhoz, hogy az x^2-es tag eltűnjön, a $w=-b/3a$ értéket kell választanunk. De a megoldásokat most nem kapjuk meg közvetlenül köbgyökvonással, mert az egyenletben benne marad általában az x-es tag! Annyit azért elértünk, hogy (az a főegyütthatóval való osztás után) az egyenlet

$$x^3+px+q=0 \tag{1.2.2}$$

alakú lesz alkalmas p-re és q-ra, amelyek az eredeti egyenlet együtthatóiból a négy alapművelet segítségével kifejezhetők. Tudjuk azt is, hogy ennek az egyenletnek a megoldásaiból az eredeti egyenlet megoldásait megkaphatjuk $b/3a$ levonásával.

1.2.2. Gyakorlat. Mutassuk meg, hogy az (1.2.1) egyenlet esetében az $x \mapsto x - b/3a$ az egyetlen olyan helyettesítés, ami eltünteti az x^2 együtthatóját. Számítsuk ki az (1.2.2) egyenletben keletkező p és q értékét is.

Tehát elegendő ezt az új egyenletet megoldanunk. A megoldáshoz vezető ötletet az alábbi azonos átalakítás szolgáltatja:

$$(u+v)^3 = u^3+3u^2v+3uv^2+v^3 = u^3+v^3+3uv(u+v)\,,$$

azaz

$$(u+v)^3 - 3uv(u+v) - (u^3+v^3) = 0\,.$$

Ez az azonosság hasonlít a megoldandó egyenlet $x^3 + px + q = 0$ alakjához. Ha sikerülne az u és v számokat úgy megválasztani, hogy a

$$\left.\begin{aligned} -3uv &= p \\ -(u^3+v^3) &= q \end{aligned}\right\} \tag{1.2.3}$$

egyenletrendszer teljesüljön, akkor $x = u + v$ biztosan az egyenlet megoldása lenne.

1.2.3. Kérdés. Beláttuk-e, hogy az $x^3 + px + q = 0$ egyenlet minden megoldása $u + v$ alakban írható, ahol u és v kielégíti ezt az egyenletrendszert?

Hogyan lehetne megoldani ezt az egyenletrendszert? Az olyan egyenletrendszereket, ahol a két ismeretlen összege és szorzata adott, másodfokú egyenletre vezethetjük vissza.

1.2.4. Gyakorlat. Mutassuk meg, hogy ha a és b valós számok, akkor az

$$\left.\begin{aligned} x + y &= a \\ xy &= b \end{aligned}\right\}$$

egyenletrendszer megoldásai éppen a $z^2 - az + b = 0$ egyenlet megoldásai.

Az (1.2.3) egyenletrendszerben u^3 és v^3 összege $-q$, szorzatuk pedig, az első egyenletet köbre emelve, $(-p/3)^3$. Ezért u^3 és v^3 a $z^2 + qz - (p/3)^3 = 0$ másodfokú egyenlet megoldásai. Ezt a másodfokú egyenletet megoldva u és v értékét köbgyökvonással állapíthatjuk meg. A számolást elvégezve az úgynevezett *Cardano-képletet* kapjuk:

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\,.$$

A négyzetgyök alatt álló $(q/2)^2 + (p/3)^3$ kifejezést általában D betűvel fogjuk jelölni.

Az 1.2.3. Kérdésre adott válasz szerint egyáltalán nem láttuk be, hogy a Cardano-képlet megadja a harmadfokú egyenlet összes gyökét. Gyanakvásra adhat okot, hogy mivel a valós számok körében minden számnak egy köbgyöke van, a képlet csak egyetlen megoldást szolgáltathat. Márpedig könnyen felírhatunk egy olyan harmadfokú egyenletet, aminek három valós megoldása van, például

$$(x-1)(x-4)(x+5) = x^3 - 21x + 20 = 0\,.$$

Vajon az 1, 4 és -5 közül melyiket adja a Cardano-képlet? Ha behelyettesítünk, akkor $D = -243$, azaz negatív szám adódik. Ebből nem tudunk négyzetgyököt vonni, tehát az egyenlet egyik megoldását sem kapjuk meg!

Használhatatlan lenne a módszerünk? Mielőtt feladnánk, vizsgáljunk meg két másik egyenletet is. Az $x^3 - 9x - 28 = 0$ esetben $D = 169$, azaz $x = \sqrt[3]{14 + 13} + \sqrt[3]{14 - 13} = 3 + 1 = 4$. Több megoldás nincs is (a valós számok között), mert

$$x^3 - 9x - 28 = (x-4)(x^2 + 4x + 7)\,,$$

és a második tényezőnek nincs valós gyöke.

Lehet, hogy ha csak egy valós megoldás van, akkor a képlet ezt mindig megadja? Az előző példán felbátorodva próbálkozzunk meg az $x^3 - 3x - 52$ egyenlettel. Az eredmény

$$x = \sqrt[3]{26 + \sqrt{675}} + \sqrt[3]{26 - \sqrt{675}}\,,$$

kalkulátorral ezt (közelítőleg) kiszámítva $x = 4$ adódik. Szorzattá alakítással most is meggyőződhetünk arról, hogy az egyenlet egyetlen valós megoldása az $x = 4$. Tehát a fenti gyökös kifejezés nemcsak közelítőleg, hanem pontosan egyenlő 4-gyel! Ezt közvetlenül is be tudjuk látni, ha észrevesszük, hogy

$$26 + \sqrt{675} = 26 + 15\sqrt{3} = 2^3 + 3 \cdot 2^2 \cdot \sqrt{3} + 3 \cdot 2\sqrt{3}^2 + \sqrt{3}^3 = (2 + \sqrt{3})^3\,,$$

és ugyanígy $26 - \sqrt{675} = (2 - \sqrt{3})^3$. Ezért $x = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4$.

Térjünk most vissza az $x^3 - 21x + 20 = 0$ egyenletből kapott

$$x = \sqrt[3]{-10 + \sqrt{-243}} + \sqrt[3]{-10 - \sqrt{-243}}$$

eredményre. Felejtsük el, hogy nincs olyan valós szám, aminek a négyzete -243, és próbáljuk most is az előző módon elvégezni a köbgyökvonást. Annyit persze elfogadunk, hogy $(\sqrt{-3})^2 = -3$. Azt kapjuk, hogy

$$-10+\sqrt{-243} = -10+9\sqrt{-3} = 2^3+3\cdot 2^2\cdot\sqrt{-3}+3\cdot 2(\sqrt{-3})^2+(\sqrt{-3})^3 = (2+\sqrt{-3})^3\,,$$

és ugyanígy $-10 - \sqrt{-243} = (2 - \sqrt{-3})^3$. Ezért $x = (2 + \sqrt{-3}) + (2 - \sqrt{-3}) = 4$.

Vagyis az egyik megoldást ki tudjuk hozni a Cardano-képletből, ha hajlandók vagyunk formálisan számolni negatív számok négyzetgyökével, mert ezek a négyzetgyökök a végén kiesnek! Sőt, a „köbgyökvonást” másképp végezve a másik két megoldás is kijön:

1.2.5. Gyakorlat. „Mutassuk meg”, hogy

$$\left(-\frac{5}{2} + \frac{\sqrt{-3}}{2}\right)^3 = \left(\frac{1}{2} - \frac{3\sqrt{-3}}{2}\right)^3 = -10 + \sqrt{-243}\,.$$

A két új „köbgyököt” felhasználva $x_2 = (-5/2 + \sqrt{-3}/2) + (-5/2 + \sqrt{-3}/2) = -5$, illetve $x_3 = (1/2 - 3\sqrt{-3}/2) + (1/2 + 3\sqrt{-3}/2) = 1$ adódik.

Találtunk egy csóválódó farkat, keressük meg a kutyát! Szabad-e, és ha igen, milyen szabályok szerint szabad számolni ezekkel az újfajta kifejezésekkel? Igaz-e, hogy a Cardano-képlettel az összes harmadfokú egyenlet megoldható? Mi lesz a megoldások száma? Van-e a fenti trükkös eljárástól különböző, mechanikus módszer a köbgyökvonás elvégzésére? Mindezekre a kérdésekre a *komplex számok* bevezetése adja meg a választ. A Cardano-képlet pontos tárgyalására a 3.8. Szakaszban térünk majd vissza.

Gyakorlatok, feladatok

1.2.6. Kérdés. Elérhetjük-e alkalmas $x \to x + w$ helyettesítéssel, hogy az (1.2.1) harmadfokú egyenletből az x-es tag, illetve a konstans tag (vagyis a d) tűnjön el?

1.2.7. Kérdés. Helyes-e az 1.2.4. Gyakorlatra adott következő megoldás? Ha $x + y = a$ és $xy = b$, akkor $(z - x)(z - y) = z^2 - (x + y)z + xyz = z^2 - az + b$. Tehát a $z^2 - az + b$ egyenletnek megoldása x is és y is.

1.2.8. Gyakorlat. Melyik természetes számmal egyenlő $\sqrt[3]{7 + \sqrt{50}} + \sqrt[3]{7 - \sqrt{50}}$?

1.2.9. Gyakorlat. „Mutassuk meg", hogy $\sqrt[4]{-4} = 1 + \sqrt{-1}$. Keressük meg $\sqrt[4]{-4}$ három további értékét is.

1.2.10. Gyakorlat. Egy pozitív valós számból két négyzetgyök vonható. Ezért ha D értéke pozitív, akkor látszólag a Cardano-képletből négy megoldást nyerhetünk (hiszen mindkét négyzetgyökvonásnak kétféle eredménye lehet). Hogy lehet ez? Tényleg négy megoldása van ilyenkor a harmadfokú egyenletnek?

1.2.11. Gyakorlat. Az alábbi levezetés ellentmondáshoz vezet:

$$1 = \sqrt{1} = \sqrt{(-1) \cdot (-1)} = \sqrt{-1} \cdot \sqrt{-1} = -1\,.$$

Fel kell adnunk a $\sqrt{-1}$-et tartalmazó kifejezésekkel való számolás gondolatát?

1.2.12. Feladat. Igazoljuk Bolzano tételének[1] felhasználásával, hogy egy valós együtthatós harmadfokú egyenletnek mindig van valós megoldása.

1.3. Számolás komplex számokkal

A tervünk az, hogy olyan kifejezésekkel is tudjunk formálisan számolni, melyekben negatív számok négyzetgyökei is szerepelnek. Az 1.2.11. Gyakorlat azonban óvatosságra int. Meg kell pontosan mondanunk, milyen kifejezéseket akarunk vizsgálni, és megállapítani a számolás szabályait.

Hogy ne kelljen sokat írni, vezessük be a $\sqrt{-1} = i$ rövidítést. Látni fogjuk, hogy hasonló rövidítést nem kell bevezetnünk a többi negatív szám négyzetgyökére, például $\sqrt{-4}$ helyett írhatunk majd $2\sqrt{-1} = 2i$-t, mert e két szám négyzete ugyanaz. Mivel az összeadást és a szorzást is el akarjuk végezni, biztosan meg kell engednünk az olyan kifejezéseket, mint például $3 + 2i$, vagyis általában az $a + bi$ alakú kifejezéseket, ahol a és b valós számok. Ezekkel úgy fogunk számolni, mintha i egy ismeretlen lenne, de közben felhasználhatjuk, hogy $i^2 = \sqrt{-1}^2 = -1$.

[1] Az analízisből ismert Bolzano-tétel (lásd A.0.2. Tétel) azt mondja ki, hogy ha egy folytonos függvény (mint például az (1.2.1) egyenlet bal oldala) bizonyos helyeken negatív, illetve pozitív értéket vesz fel, akkor e két hely között felveszi a nulla értéket is, azaz „valahol át kell metszenie az x-tengelyt".

Tegyük fel, hogy az $a + bi$ alakú kifejezésekkel szabad a szokásos szabályok szerint számolni. Ekkor két ilyen kifejezést könnyű összeadni:

$$(a + bi) + (c + di) = (a + c) + (b + d)i \, .$$

Sőt, össze is tudjuk szorozni őket:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \, ,$$

hiszen $i^2 = -1$.

1.3.1. Kérdés. Át lehet-e olyan ravaszul alakítani a $2 + 3i$ kifejezést, hogy a végén $4 + 5i$ jöjjön ki?

Eddig a lehetőségeinket vizsgálgattuk, azt, hogy *ha* sikerülne számolni a negatív számok négyzetgyökeivel, akkor milyen szabályok kötnének bennünket. Most már eleget tudunk ahhoz, hogy végre *definiálhassuk* a komplex számokat.

1.3.1. Definíció. *Komplex számoknak* az $a+bi$ alakú formális kifejezéseket nevezzük, ahol a és b valós számok. Az $a + bi$ és a $c + di$ számokat akkor tekintjük egyenlőnek, ha $a = c$ és $b = d$. A komplex számok $\mathbb{C}$ halmazán az alábbi képletekkel definiáljuk az összeadást és a szorzást:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \, .$$

Emlékeztetőül megjegyezzük, hogy az egész, racionális, illetve valós számok halmazát rendre $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ jelöli.

Az 1.3.1. Kérdésre adott válasz megmutatja, hogy miért így definiáltuk komplex számok egyenlőségét, az előtte levő számolás pedig, hogy miért így definiáljuk a műveleteket. Definíciónk alkalmas arra, hogy a komplex számokkal számolni tudjunk, ami most az elsődleges célunk. Matematikai szempontból azonban nem kielégítő, mert nem eléggé precíz, és mert nem mutattuk meg, hogy a számolásokból nem jöhet ki ellentmondás. Az 1.6. Szakaszban visszatérünk majd ezekre a kérdésekre, és bepótoljuk a hiányosságokat.

Ha az $a + bi$ kifejezésben $b = 0$, akkor csak a-t írunk, és így láthatjuk, hogy a valós számok mind komplex számok is egyúttal (és komplex számként persze ugyanúgy kell őket összeadni és szorozni, mint valós számként). Hasonlóképpen $0 + bi$ helyett csak bi-t fogunk írni. Az ilyen alakú komplex számokat *(tisztán) képzetes*, vagy *imaginárius* számoknak nevezzük. A $z = a + bi$ komplex szám *valós része* $\mathrm{Re}(z) = a$, *képzetes része* pedig $\mathrm{Im}(z) = b$ (a jelölés a latin eredetű "reális rész", illetve "imaginárius rész" kifejezésekből származik). Külön is felhívjuk a figyelmet arra, hogy a képzetes rész valós szám, tehát b, és nem bi.

Foglaljuk össze azokat a szabályokat, amelyek a most definiált műveletekre érvényesek. Érdemes észrevenni, hogy ezek mennyire hasonlítanak mind a valós számok körében megszokott szabályokhoz, mind pedig a maradékokkal való számolás szabályaihoz, amiket az 1.1.2. Állításban soroltunk fel.

1.3.2. Állítás. *Tetszőleges $x, y, z \in \mathbb{C}$ számokra érvényesek az alábbiak.*

(1) $(x + y) + z = x + (y + z)$ *(az összeadás asszociatív).*
(2) $x + y = y + x$ *(az összeadás kommutatív).*
(3) $x + 0 = 0 + x = x$ *(azaz létezik nullelem).*
(4) *Minden x-nek van ellentettje, azaz olyan y, melyre $x + y = y + x = 0$. (Ha $x = a + bi$, akkor ilyen y lesz $-a + (-b)i$.)*
(5) $(xy)z = x(yz)$ *(a szorzás asszociatív).*
(6) $xy = yx$ *(a szorzás kommutatív).*
(7) $x \cdot 1 = 1 \cdot x = x$ *(azaz létezik egységelem).*
(8) $(x + y)z = xz + yz$ *(disztributivitás).*

Ezt az állítást nem bizonyítjuk be, mert következni fog a később tanultakból. Egy mintabizonyítást azonban érdemes mindenkinek önállóan elvégezni.

1.3.2. Gyakorlat. Mutassuk meg a fenti azonosságok közül a disztributivitást.

Mivel minden komplex számnak van ellentettje, az 1.1. Szakaszban írottak szerint a kivonást is el tudjuk végezni. Ugyanitt láttuk azt is, hogy az osztás elvégzéséhez azt kell megvizsgálnunk, mely komplex számoknak van reciproka.

1.3.3. Gyakorlat. Keressük meg az $1 + i$ komplex szám reciprokát, vagyis azt a z komplex számot, melyre $(1 + i)z = 1$.

Noha e gyakorlatot egyenletrendszer segítségével is megoldhatjuk, eljárhatunk elegánsabban is. Az osztást a tört alkalmas bővítésével érdemes elvégezni:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\,.$$

A nevezőben szereplő $a^2 + b^2$ kifejezés mindig pozitív, kivéve ha $a = b = 0$, hiszen nem nulla valós szám négyzete pozitív. Ezért a fenti számolás mindig elvégezhető, ha a és b egyike nem nulla. A komplex számok egyenlőségének definíciója alapján viszont $a + bi$ akkor nulla, ha $a = b = 0$, és így a kapott képlet minden nem nulla komplex szám esetében értelmes.

1.3.3. Állítás. *A komplex számok között minden nem nulla számmal lehet osztani.*

Bizonyítás. Beszorzással ellenőrizhető, hogy

$$(a+bi)\left(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\right) = 1\,,$$

és így tényleg az $a + bi$ szám reciprokát kaptuk. □

1.3.4. Következmény. *A komplex számok között egy szorzat csak akkor lehet nulla, ha valamelyik tényezője nulla. (Ezt a tulajdonságot most is nullosztómentességnek nevezzük.)*

Bizonyítás. Tegyük fel, hogy $zw = 0$, de $z \neq 0$. Meg kell mutatnunk, hogy akkor $w = 0$. Mivel $z \neq 0$, van reciproka, vagyis egy olyan u, melyre $uz = 1$. Ekkor

$$w = 1 \cdot w = (uz)w = u(zw) = u \cdot 0 = 0\,.$$

Tehát $\mathbb{C}$ valóban nullosztómentes. □

Az a kifejezés, amivel osztáskor a törtet bővítettük, olyan fontos, hogy önálló nevet kapott. A $z = a + bi$ komplex szám *konjugáltjának* a $\overline{z} = a - bi$ számot nevezzük. Tehát *az osztás konkrét elvégzésekor a nevező konjugáltjával érdemes bővíteni.* A nevezőben ilyenkor a $z\overline{z} = a^2 + b^2$ kifejezés keletkezik, amiről láttuk, hogy nemnegatív valós szám.

1.3.4. Gyakorlat. Mutassuk meg, hogy ha z valós szám, akkor $\sqrt{z\overline{z}}$ a z abszolút értéke.

Ezt az észrevétel lehetővé teszi, hogy az abszolút érték fogalmát komplex számokra is kiterjesszük. A következő szakaszban egy újabb, geometriai indokot is fogunk látni arra, hogy miért érdemes a komplex számok abszolút értékét az alábbi módon definiálni.

1.3.5. Definíció. A $z = a + bi$ komplex szám konjugáltján a $\overline{z} = a - bi$ komplex számot, abszolút értékén a $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$ nemnegatív valós számot értjük.

Nagyon fontos megértenünk, hogy komplex számok között már *nem igaz, hogy az abszolút érték mindig a szám maga, vagy az ellentettje* (ami valósakra igaz volt). Komplex számok között *egyenlőtlenségeket sem írhatunk fel* (kivéve, ha véletlenül valósak), tehát nem beszélhetünk például pozitív komplex számokról. Ennek okát később (az 5.7. Szakaszban) fogjuk majd látni. Most összefoglaljuk a konjugálás és az abszolút érték néhány tulajdonságát. Ezek közül többen emlékeztetnek arra, amit az 1.1.3. Állításban műveletartásnak neveztünk.

1.3.6. Állítás. *Tetszőleges $z, w \in \mathbb{C}$ számokra érvényesek az alábbiak.*

(1) *A konjugálás kölcsönösen egyértelmű, és $\overline{\overline{z}} = z$.*
(2) *$z = \overline{z}$ akkor és csak akkor, ha z valós.*
(3) *$\overline{z + w} = \overline{z} + \overline{w}$ (a konjugálás összegtartó).*
(4) *$\overline{zw} = \overline{z}\ \overline{w}$ (a konjugálás szorzattartó).*
(5) *$|z| = 0$ akkor és csak akkor, ha $z = 0$.*
(6) *$|\overline{z}| = |z|$.*
(7) *$|zw| = |z||w|$ (az abszolút érték szorzattartó).*

Bizonyítás. Az állítások mindegyikét könnyen be lehet látni úgy, hogy a $z = a + bi$ és $w = c + di$ helyettesítés után elvégezzük a műveleteket. Ezeket a számolásokat az olvasóra hagyjuk, és csak annak a megmutatására szorítkozunk, hogy az abszolút érték szorzattartása hogyan következik abból, hogy a konjugálás szorzattartó. Nyilván

$$|zw|^2 = zw\ \overline{zw} = zw\ \overline{z}\ \overline{w} = z\overline{z}w\overline{w} = |z|^2|w|^2\,.$$

Mivel az abszolút érték nemnegatív, négyzetgyököt vonhatunk. □

Zárásként hadd említsük meg, hogy a komplex számokat nemcsak az algebrában használják. Egyes geometriai alakzatok sokkal jobban megérthetők, ha a leírásukra komplex változókat is használunk (az alakzat „valósban fekvő darabja” csupán a jéghegy csúcsa). A kvantummechanikában komplex értékű valószínűségek adják meg a részecskék állapotát. Az univerzum egyes modelljeiben az időt komplex szám jeleníti meg. Később megmutatjuk, hogy mi a komplex számoknak az a „nagyon jó” tulajdonsága, ami több ilyen alkalmazást lehetővé tesz.

Gyakorlatok, feladatok

1.3.5. Gyakorlat. Számítsuk ki az alábbi kifejezések értékét.

(1) $(1+i)(3-2i)$, $1/i$, $(1+i)/(3-2i)$.
(2) $|\overline{(4+i)}/(4+i)|$, $|(1+1526i)^{100}/(1-1526i)^{100}|$.
(3) $(1+i)^2$, $(1+i)^{1241}$.

1.3.6. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között.

(1) $x^2+1=0$.
(2) $x^2=-12$.
(3) $x^2+2x+2=0$.
(4) $x^2+2ix-1=0$.

1.3.7. Feladat. Határozzuk meg azokat a $c+di$ számokat (c és d valós), melyek négyzete $20i-21$. Oldjuk meg az $x^2+(i-2)x+(6-6i)=0$ egyenletet a komplex számok körében. E példa alapján adjunk általános eljárást a négyzetgyökvonásra, és a másodfokú egyenlet megoldására.

1.3.8. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között.

(1) $x^2=i$.
(2) $x^2+3x+4=0$.
(3) $x^2-(2+i)x+7i-1=0$.
(4) $(2+i)x^2-(5-i)x+2-2i=0$.
(5) $x=(3+2i)\overline{x}$.
(6) $x=2\cdot\mathrm{Re}(x)$.

1.3.9. Gyakorlat. Mutassuk meg, hogy a konjugálás szorzattartó.

1.3.10. Gyakorlat. Melyek igazak az alábbi állítások közül?

(1) A konjugálás tartja a kivonást.
(2) Az abszolút érték tartja az összeadást.
(3) Az abszolút érték tartja az osztást.

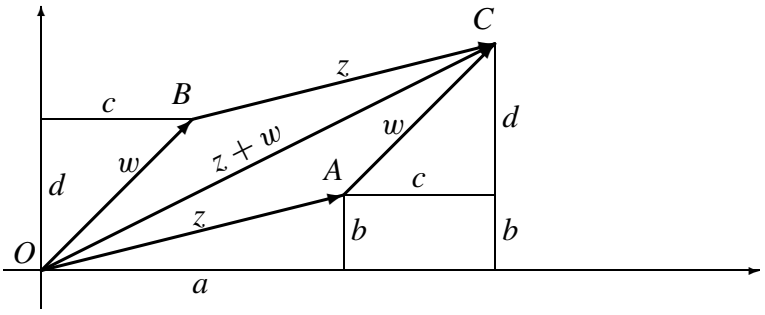
1.4. A komplex számok trigonometrikus alakja

A komplex számokat egyenletek megoldására akartuk használni. Ehhez a négy alapműveleten kívül gyökvonásra biztosan szükség van. Az 1.3.7. Feladat megoldásakor láttuk, hogy a komplex számok jobbak, mint a valósak a négyzetgyökvonás szempontjából, mert itt minden számból lehet négyzetgyököt vonni. Azt is láttuk azonban, hogy ez eléggé komplikált számolással jár, és a módszer már a köbgyökvonás elvégzéséhez is használhatatlanul bonyolultnak tűnik.

Az ilyen zsákutcákból a matematikában nem egyszer úgy kecmergünk ki, hogy félretesszük az eredeti problémát, és egy másik, látszatra teljesen új témával kezdünk foglalkozni. Gyakran megesik, hogy ennek során váratlanul ötleteket kapunk az eredeti probléma megválaszolására is. Most is ezt az utat követjük, és „melléktermékként” nemcsak a gyökvonás módszerét fedezzük fel, hanem geometriai feladatok megoldásához is hasznos eszközre lelünk.

Az új téma amivel foglalkozunk, a következő: ha a valós számokat a számegyenesen tudjuk ábrázolni, akkor érdemes-e a komplex számokat is hasonló módon lerajzolni? A tapasztalatok azt mutatják, hogy erre a sík bizonyul alkalmasnak. Írjuk rá az $a+bi$ számot a sík (a,b) pontjára. Ez azért hasznos, mert a komplex számok műveletei nagyon ismerősek lesznek geometriából!

Akár fizikából, akár geometriából, mindannyian ismerjük a *vektorok* fogalmát. Foglaljuk össze, mit is tudunk ezekről. A vektorokat az irányított szakaszokból kapjuk úgy, hogy az egyenlő hosszú és egyforma állású irányított szakaszokat egyenlőnek, ugyanannak a vektornak tekintjük. Ezért néha érdemes csak azokat a szakaszokat vizsgálni, amelyek kezdőpontja az origóban van. Ekkor *helyvektorokról* beszélünk. A helyvektorokat szokás a végpontjukkal azonosítani, vagyis a sík (a,b) pontját vektornak is tekinthetjük: annak a vektornak, ami az origóból (a,b)-be mutat.

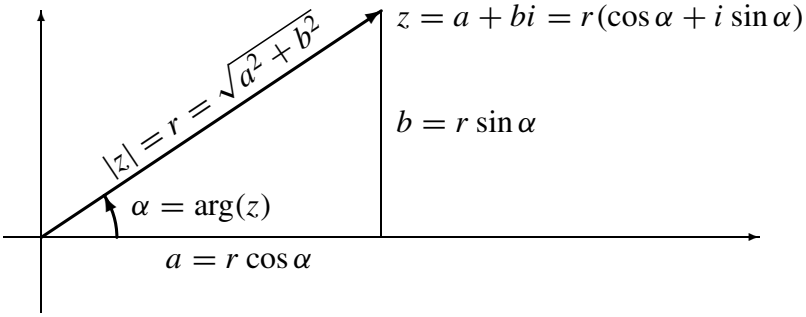


1.4.1. ábra. Vektorösszeadás

Vektorokat úgy adunk össze, hogy egymás után fűzzük őket. Helyvektorok esetében ezt úgy lehet lefordítani, hogy az A és B pontba mutató vektorok összege akkor mutat a C pontba, ha az $OACB$ négyszög paralelogramma. Ha kiszámoljuk a koordinátákat, akkor ebből az adódik, hogy az (a,b) és (c,d) helyvektorok összege $(a+c,b+d)$. Vegyük észre, hogy ugyanezzel a képlettel kell összeadni a komplex számokat is!

1.4.1. Állítás. *A komplex számok összeadása a vektorösszeadásnak felel meg. Pontosabban: két komplex szám összegének megfelelő helyvektor a két komplex számnak megfelelő helyvektorok összege.*

A komplex számok szorzásának képlete első ránézésre nem utal geometriai kapcsolatra. Ahhoz, hogy a kapcsolatot felfedezzük, érdemes észrevenni, hogy minden nem nulla helyvektort egyértelműen meghatároz az origótól való távolsága, vagyis a *hossza*, továbbá az x-tengely pozitív felétől mért, irányított *szöge*. Például az $1 - i$ szöge 315° (vigyázzunk, nem 45°). A z komplex szám szögét néha z árkuszának vagy *argumentumának* is nevezik, és ilyenkor $\arg(z)$-vel jelölik. Ez a szög egyértelműen meghatározott, ha kikötjük, hogy $0 \le \arg(z) < 2\pi = 360^\circ$ legyen.



1.4.2. ábra. Komplex szám trigonometrikus alakja

Az 1.4.2. ábrából leolvashatjuk a következő összefüggéseket. Ha a $z = a + bi \neq 0$ szám hossza r és szöge α, akkor nyilván

$$a = r\cos\alpha \qquad \text{és} \qquad b = r\sin\alpha\,,$$

azaz $z = r\cos\alpha + ir\sin\alpha = r(\cos\alpha + i\sin\alpha)$. Ezt a felírást a $z \neq 0$ szám *trigonometrikus alakjának*, a $z = a + bi$ felírást *algebrai alaknak* nevezzük. Vegyük észre, hogy

$$|z|^2 = a^2 + b^2 = r^2(\cos^2\alpha + \sin^2\alpha) = r^2\,,$$

azaz *komplex szám hossza ugyanaz, mint az abszolút értéke*. Mindezt persze leolvashatjuk az ábráról is, ha Pitagorasz tételét alkalmazzuk. A nulla komplex számnak sem szöge, sem trigonometrikus alakja nincs.

1.4.2. Tétel. *Tetszőleges z és w komplex számokra $|z + w| \le |z| + |w|$ teljesül. Ezt* háromszög-egyenlőtlenségnek nevezzük. *Egyenlőség akkor van, ha z és w párhuzamosak, és egyenlő állásúak.*

Bizonyítás. Ha a z és w vektorokat összefűzéssel adjuk össze, akkor egy olyan OAC háromszöget kapunk, melyre $\overrightarrow{OA} = z$, $\overrightarrow{AC} = w$ és $\overrightarrow{OC} = z + w$. Vagyis az állítás valóban a háromszögegyenlőtlenségnek felel meg. Egyenlőség akkor van, ha háromszög elfajuló, mégpedig úgy, hogy az A csúcs az OC szakaszra esik. □

A háromszög-egyenlőtlenséget algebrailag is be lehet bizonyítani, ha z-t és w-t algebrai alakban írjuk fel, és átrendezünk. Ekkor a híres Cauchy-Bunyakovszkij-Schwarz egyenlőtlenségre vezethetjük vissza az állítást. Ez a kapcsolat, és mindkét egyenlőtlenség sokkal általánosabban, úgynevezett euklideszi vektorterekben is teljesül. Az érdeklődő olvasó a [**3**] könyv 8.2. Szakaszában nézhet mindennek utána.

A trigonometrikus alak jelentőségét akkor érthetjük meg igazán, ha ilyen alakban szorozzuk össze a komplex számokat. Legyen $z = r(\cos\alpha + i\sin\alpha)$ és $w = s(\cos\beta + i\sin\beta)$. Ekkor

$$zw = rs(\cos\alpha\cos\beta - \sin\alpha\sin\beta) + rs(\cos\alpha\sin\beta + \sin\alpha\cos\beta)i\ ,$$

ami az ismert addíciós képletek miatt $rs(\cos(\alpha+\beta) + i\sin(\alpha+\beta))$. Látszólag tehát beláttuk, hogy *komplex számok szorzásakor hosszuk összeszorzódik, szögük összeadódik.* Azt eddig is tudtuk, hogy az abszolút érték szorzattartó, a szögekre vonatkozó észrevétel azonban új.

Itt azonban valamire vigyáznunk kell. Komplex szám szögét 0 és 360° fok közöttinek definiáltuk. A most kapott képlet tehát szigorúan véve nem mindig trigonometrikus alak, mert az $\alpha+\beta$ szög túllépheti a 360 fokot. Például ha $-i$-t, aminek a hossza 1, szöge 270°, önmagával szorozzuk, akkor a fenti képletből a

$$(-i)^2 = \cos 540^\circ + i\sin 540^\circ$$

adódik. Ez persze ugyanaz, mint $\cos 180^\circ + i\sin 180^\circ = -1$, hiszen a sin és a cos függvény is 360° szerint periodikus. A legegyszerűbben úgy szabadulhatunk meg ettől a problémától, ha a trigonometrikus alakban megengedünk tetszőleges szöget, de ennek ára az, hogy a trigonometrikus alakban szereplő szög csak „modulo 360°" lesz egyértelmű.

1.4.1. Gyakorlat. Mutassuk meg, hogy

$$r(\cos\alpha + i\sin\alpha) = s(\cos\beta + i\sin\beta) \neq 0$$

akkor és csak akkor, ha $r = s \neq 0$, és $\alpha - \beta$ a 360° egész számú többszöröse.

Most már pontosan megfogalmazhatjuk a szorzás szabályát is.

1.4.3. Állítás. *Komplex számok szorzásakor hosszuk összeszorzódik, szögük pedig összeadódik modulo* 360°. *A* $z = r(\cos\alpha + i\sin\alpha) \neq 0$ *számmal való szorzás tehát forgatva nyújtás: az origó körül* α *szöggel forgat, és az origóból* r*-szeresre nyújt.*

A komplex számok azért előnyösebbek a geometriai feladatok megoldásakor, mint a vektorok, mert nemcsak a vektorösszeadást, hanem a forgatásokat és nyújtásokat is fel lehet írni velük, méghozzá könnyebben kezelhető formában, mintha koordináta-geometriával számolnánk. A fejezet végén több feladattal próbáljuk meg illusztrálni ezeket az előnyöket.

1.4.2. Gyakorlat. Adjunk képletet két komplex szám hányadosára a trigonometrikus alak felhasználásával.

A szorzásra levezetett képlet segítségével hatványozni is tudunk, hiszen az ismételt szorzás. Nevezetesen

$$[r(\cos\alpha + i\sin\alpha)]^n = r^n(\cos n\alpha + i\sin n\alpha)\,.$$

Ezt az összefüggést *Moivre képletének* nevezzük. (Sokszor így hívják a trigonometrikus alakban felírt számok szorzásának szabályát is.) Hatványozáskor tehát a szöget a kitevővel kell szorozni, a hosszat pedig a kitevőre kell emelni. Ha a valós számokhoz hasonlóan a hatványozást negatív egész kitevőkre is kiterjesztjük, vagyis z^0 értékét 1-nek, z^{-n} értékét pedig $1/z^n$-nek definiáljuk, akkor az 1.4.2. Gyakorlat alapján könnyű meggondolni, hogy Moivre képlete minden egész kitevőre érvényes lesz.

Gyakorlatok, feladatok

1.4.3. Gyakorlat. Ha z és w komplex számok, mi a geometriai jelentése a $\overline{z}$ számnak, a $z-w$ vektornak, illetve a $|z-w|$ számnak?

1.4.4. Gyakorlat. Rajzoljuk le a komplex számsíkon a következő halmazokat:

(1) $\{z\in\mathbb{C} : \mathrm{Re}(z+3+2i)\le -2\}$.
(2) $\{z\in\mathbb{C} : \mathrm{Re}(z+1)\ge \mathrm{Im}(z-3i)\}$.
(3) $\{z\in\mathbb{C} : |z-i-1|\le 3\}$.
(4) $\{z\in\mathbb{C} : |z-3+2i| = |z+4-i|\}$.
(5) $\{z\in\mathbb{C} : z+\overline{z} = -1\}$.
(6) $\{z\in\mathbb{C} : 1/z = \overline{z}\}$, illetve $\{z\in\mathbb{C} : (1/z)+8 = \overline{z}\}$.
(7) $\{z\in\mathbb{C} : |z| = iz\}$.
(8) $\{z\in\mathbb{C} : \mathrm{Im}((z-1)/(z+1)) = 0\}$, illetve $\{z\in\mathbb{C} : \mathrm{Re}((z-1)/(z+1)) = 0\}$.

1.4.5. Gyakorlat. Írjuk fel az alábbi komplex számokat trigonometrikus alakban:

(1) $1+i$ és $1-i$.
(2) $\sqrt{3}+i$ és $-1-\sqrt{3}i$.
(3) $\cos(60^\circ) - i\sin(60^\circ)$.
(4) $\cos(30^\circ) - i\sin(60^\circ)$.

1.4.6. Gyakorlat. A sík mely geometriai transzformációinak felelnek meg a komplex számok halmazának alábbi leképezései:

(1) $z\to 3z+2$.
(2) $z\to (1+i)z$.
(3) $z\to 1/\overline{z}$.

1.4.7. Gyakorlat. Legyenek $z=a+bi$ és $w=c+di$ különböző komplex számok. Írjuk fel az alábbi „alakzatok egyenletét” komplex számok segítségével. Az eredményben ne szerepeljen a, b, c, d, csak z és w.

(1) A z-t w-vel összekötő szakasz felezőpontja.
(2) A z-t w-vel összekötő szakasz felező merőlegese.

(3) A z középpontú, w-t tartalmazó körvonal.
(4) Az origóból z-be mutató vektor $+90$ fokos elforgatottja.
(5) A w-ből z-be mutató vektor $+90$ fokos elforgatottja.
(6) A z pont w körüli $+90$ fokos elforgatottja.
(7) Annak a négyzetnek a csúcsai, amelynek a z-t w-vel összekötő szakasz átlója.
(8) Annak a két szabályos háromszögnek a középpontja, melyeknek az adott két szám két csúcsa.

1.4.8. Feladat. Egy négyszög oldalaira kifelé négyzeteket rajzolunk. Kössük össze az átellenes oldalakra rajzolt négyzetek középpontjait. Mutassuk meg, hogy az így kapott két szakasz merőleges, és egyenlő hosszú.

1.4.9. Feladat. Írjunk egy háromszög mindegyik oldalára kifelé egy szabályos háromszöget. Igazoljuk, hogy ezek középpontjai szabályos háromszöget alkotnak.

1.4.10. Feladat. Mutassuk meg, hogy a z_1, z_2, z_3, z_4 páronként különböző komplex számok akkor és csak akkor vannak egy körön vagy egyenesen, ha kettősviszonyuk, vagyis a

$$(z_1\, z_2\, z_3\, z_4) = \frac{z_3 - z_1}{z_3 - z_2} \Big/ \frac{z_4 - z_1}{z_4 - z_2}$$

kifejezés valós szám.

1.4.11. Feladat. Igazoljuk Ptolemaiosz tételét: ha egy négyszög oldalainak hossza rendre a, b, c, d, átlóinak hossza pedig e és f, akkor $ac + bd \geq ef$, és egyenlőség akkor és csak akkor áll, ha a négyszög (konvex) húrnégyszög.

1.4.12. Feladat. Hozzuk zárt alakra a $\sin x + \sin 2x + \cdots + \sin nx$ összeget.

1.5. Egységgyökök és rendjeik

Moivre képlete alapján már el tudjuk végezni komplex számok között a gyökvonást. Ehhez a megoldást trigonometrikus alakban keressük. Ha tehát $z = r(\cos\alpha + i\sin\alpha)$ nem nulla szám, és $n \geq 1$ egész, akkor olyan w számot keresünk, amelyre $w^n = z$. Azonnal láthatjuk, hogy $w_0 = \sqrt[n]{r}(\cos(\alpha/n) + i\sin(\alpha/n))$ jó lesz, hiszen ezt a számot n-edik hatványra emelve z-t kapjuk vissza.

1.5.1. Kérdés. Ahhoz, hogy w_0 értékét kiszámítsuk, n-edik gyököt kell vonni r-ből. Miért egyszerűbb dolog ez, mint egy általános komplex számból vonni n-edik gyököt?

A z szám *összes* n-edik gyökét közvetlen számolással is megkereshetjük.

1.5.2. Gyakorlat. Igazoljuk, hogy a $z = r(\cos\alpha + i\sin\alpha)$ szám n-edik gyökei pontosan a

$$w = \sqrt[n]{r}\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right)$$

alakú számok, ahol $0 \leq k < n$ egész szám.

A közvetlen számolás helyett a következőképpen is eljárhatunk. Legyen w a z tetszőleges n-edik gyöke. A fenti w_0 számra ekkor $w_0^n = z = w^n$, ahonnan $(w/w_0)^n = 1$. Jelöljük a w/w_0 hányadost ε-nal, akkor tehát $\varepsilon^n = 1$. Így ha sikerülne meghatározni az ilyen ε számokat, akkor az összes keresett w-t is megkapnánk a $w = \varepsilon w_0$ összefüggésből.

1.5.1. Definíció. Az $\varepsilon \in \mathbb{C}$ számot n-edik *komplex egységgyök*nek nevezzük, ha $\varepsilon^n = 1$.

Például az i szám negyedik egységgyök, hiszen $i^2 = -1$, és ezért $i^4 = 1$. Az i szám hatványai tehát

$$\begin{array}{cccccccc} i^1, & i^2, & i^3, & i^4, & i^5, & i^6, & i^7, & i^8, \quad \dots \\ \hline i, & -1, & -i, & 1, & i, & -1, & -i, & 1, \quad \dots \end{array}$$

Vagyis a hatványok periodikusan ismétlődnek. Ha lerajzoljuk őket, egy négyzetet kapunk, melynek a középpontja az origó, és az egységkörbe írható. Ezeket az észrevételeket rövidesen általánosítani fogjuk, és akkor az is kiderül majd, hogy az i, -1, $-i$, 1 számok az 1 szám *összes* negyedik gyöke, vagyis az összes negyedik egységgyök.

Az n-edik egységgyököket trigonometrikus alakban keressük meg. Mivel $\varepsilon^n = 1$, és az abszolút érték szorzattartó, $|\varepsilon|^n = 1$, azaz $|\varepsilon| = 1$. Tehát $\varepsilon = \cos\alpha + i\sin\alpha$, és így

$$\cos n\alpha + i\sin n\alpha = \varepsilon^n = 1 = 1(\cos 0 + i\sin 0)\,.$$

Az 1.4.1. Gyakorlat miatt $n\alpha = 2k\pi$ alkalmas k egészre. Tehát $\alpha = 2k\pi/n$.

1.5.2. Tétel. *Az n-edik egységgyökök száma pontosan n, ezek az*

$$\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n) = \varepsilon_1^k$$

képlettel definiált $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n = 1$ számok. Ha $z = r(\cos\alpha + i\sin\alpha)$ nem nulla komplex szám, akkor egyik n-edik gyöke

$$w_0 = \sqrt[n]{r}(\cos(\alpha/n) + i\sin(\alpha/n))\,,$$

a többi n-edik gyökét pedig úgy kapjuk meg, hogy a w_0 számot végigszorozzuk az n-edik egységgyökökkel. Minden nem nulla komplex számnak pontosan n darab n-edik gyöke van a komplex számok között, és ezek egy origó középpontú szabályos sokszög csúcsaiban helyezkednek el.

Bizonyítás. Ha lerajzoljuk az $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n = 1$ számokat a síkon, akkor egy szabályos n-szöget kapunk, amelynek természetesen mind különbözők a csúcsai. Viszont $\varepsilon_{n+1} = \varepsilon_1$, $\varepsilon_{n+2} = \varepsilon_2$, és így tovább, vagyis körbe-körbe járunk a szabályos n-szög csúcsain. Általában ha k-nak az n-nel való osztási maradéka r, akkor nyilván $\varepsilon_k = \varepsilon_r$. Az $\varepsilon_k = \varepsilon_1^k$ összefüggés nyilvánvalóan következik Moivre képletéből. Végül a z szám n-edik gyökei azért alkotnak szabályos n-szöget, mert ez w_0-lal szorzással, azaz forgatva nyújtással kapható az egységgyökök által alkotott sokszögből. □

Az n-edik komplex egységgyököket „ugyanúgy kell szorozni, ahogy a modulo n maradékokat összeadni”. Valóban, amikor az ε_k és ε_ℓ számokat szorozzuk össze, akkor a szögeket modulo 360° kell összeadni, és ezért az indexek modulo n adódnak össze. Képlettel felírva:

$$\varepsilon_{k+n\ell} = \varepsilon_k \varepsilon_\ell \,.$$

Még máshogy fogalmazva a $k \mapsto \varepsilon_k$ leképezés (kölcsönösen egyértelmű, és) művelettartó a $\mathbb{Z}_n$ halmaz és az n-edik egységgyökök halmaza között akkor, ha az első esetben a modulo n összeadást, a másodikban pedig a komplex számok szorzását tekintjük műveletnek. (De mondhatjuk azt is, hogy a $\mathbb{Z}$-ből $\mathbb{C}$-be vezető $k \mapsto \varepsilon_k$ leképezés művelettartó, ha az első művelet az összeadás, a második a szorzás, hiszen $\varepsilon_{k+\ell} = \varepsilon_k \varepsilon_\ell$ is teljesül. Ez a leképezés azonban már nem kölcsönösen egyértelmű.)

A fejezet hátralévő részében a komplex szám *rend*jének a fogalmával ismerkedünk meg. Ez a téma kicsit nehezebb az eddigieknél, ezért az olvasó megteheti, hogy előreszalad a polinomokhoz, és ide akkor tér vissza, amikor már kicsit jobban beleszokott az új gondolkodásmódba. A most következő anyagra legközelebb a körosztási polinomok vizsgálatakor, azután pedig a csoportelméleti elemrend tárgyalásakor lesz szükség.

Az ε_1 komplex számról beláttuk, hogy hatványai periodikusan ismétlődnek. Vizsgáljunk most meg ebből a szempontból egy tetszőleges z nem nulla komplex számot. „Tipikus esetben” a z szám összes egész kitevőjű hatványa páronként különböző lesz. Ilyen szám például a $z = 2$, hiszen az $1, 2, 4, 8, \ldots$ és $1, 1/2, 1/4, 1/8, \ldots$ számok között nincs két egyenlő.

1.5.3. Kérdés. Mely valós $z \neq 0$ számokra fordulhat elő, hogy $z^k = z^\ell$, noha $k \neq \ell$?

Tegyük fel, hogy z-nek vannak egyenlő hatványai is: $z^k = z^\ell$, noha $k \neq \ell$. Ekkor $z^{k-\ell} = z^{\ell-k} = 1$, így vannak olyan kitevők, melyekre z-t emelve 1-et kapunk. Ezeket hívjuk *jó* kitevőknek.

$$\boxed{n \text{ jó kitevője } z\text{-nek, ha } z^n = 1.}$$

Mivel a $k - \ell$ és $\ell - k$ jó kitevők egyike pozitív, van pozitív jó kitevő is. Legyen d a *legkisebb* pozitív jó kitevő. Osszuk el $k - \ell$-et maradékosan d-vel: $k - \ell = dq + r$, ahol $0 \leq r < d$. Ekkor

$$1 = z^{k-\ell} = z^{dq+r} = (z^d)^q z^r = 1^q z^r = z^r \,.$$

Tehát r is jó kitevő. Mivel d a legkisebb pozitív jó kitevő volt, és $r < d$, az r már nem lehet pozitív. Ezért $r = 0$, vagyis $d \mid k - \ell$. Beláttuk tehát, hogy ha $z^k = z^\ell$, akkor $d \mid k - \ell$.

Ennek az állításnak a megfordítása is igaz. Ha $d \mid k - \ell$, akkor $z^{k-\ell}$ hatványa $z^d = 1$-nek, és így $z^{k-\ell} = 1$, vagyis $z^k = z^\ell$. Szavakban megfogalmazva: z két hatványa akkor és csak akkor egyenlő, ha a kitevők különbsége a d szám többszöröse.

Tehát z hatványai d szerint periodikusak! Hiszen $z, z^2, \ldots, z^d = 1$ még páronként különböző (mert e d-nél kisebb kitevők különbsége nem lehet d-vel osztható), de már $z^{d+1} = z$, $z^{d+2} = z^2$, és így tovább. Így z-nek pontosan d darab különböző hatványa van. Ezt a d számot a z *rendjének* nevezzük.

1.5.3. Definíció. Egy z komplex szám különböző (egész kitevős) hatványainak a számát a z *rendjének* nevezzük. Ez vagy pozitív egész, vagy ∞. A rendet $o(z)$-vel jelöljük.

1.5.4. Tétel. *A z számnak vagy bármely két egész kitevőjű hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periodikusan ismétlődnek. A rend a legkisebb pozitív „jó" kitevő, vagyis a legkisebb olyan pozitív egész, melyre a számot emelve 1-et kapunk. Továbbá*

$$\boxed{z^k = z^\ell \iff o(z) \mid k-\ell, \quad \textit{speciálisan} \quad z^k = 1 \iff o(z) \mid k.}$$

A jó kitevők tehát pontosan a rend többszörösei.

Az olvasónak *a lehető legmelegebben ajánljuk,* hogy a fentiek jobb megértése érdekében ismételje át a rendnek a számelméletben használt, analóg fogalmát (lásd például [**4**], 3.2. Szakasz). Röviden összefoglaljuk a legfontosabb tudnivalókat.

Legyen $z \in \mathbb{Z}_m$ olyan szám, amely m-hez relatív prím. Hatványozzuk z-t a modulo m szorzás szerint. A hatványok periodikusan ismétlődni fognak. Nevezzük z rendjének modulo m (jele $o_m(z)$) a z szám modulo m különböző hatványainak a számát. A rend most is a legkisebb pozitív „jó" kitevő, vagyis a legkisebb olyan pozitív egész, melyre a számot a $*_m$ szorzás szerint hatványozva 1-et kapunk. Az elemi számelméletben szívesebben használnak mindennek a kifejezésére kongruenciákat. Ezen a nyelven fogalmazva tehát tetszőleges m-hez relatív prím z egészre

$$\boxed{z^k \equiv z^\ell \ (m) \iff o_m(z) \mid k-\ell, \quad \text{speciálisan} \quad z^k \equiv 1 \ (m) \iff o(z) \mid k.}$$

A jó kitevők tehát pontosan a rend többszörösei.

Fontos észrevennünk, hogy nem minden n-edik komplex egységgyök rendje n. Például az 1 rendje 1, noha az 1 minden n-re n-edik egységgyök. A negyedik egységgyökök közül az i és $-i$ rendje 4, a -1 rendje 2, az 1 rendje pedig 1. A hatodik egységgyökök rendjeit a 3.9.1. ábrán szemléltettük (125. oldal). Próbáljuk most általánosan meghatározni az n-edik egységgyökök rendjeit. Ebben a következő feladat lesz a segítségünkre.

1.5.4. Feladat. Egy bolha ugrál körbe egy n-szög csúcsain, úgy, hogy minden ugrásnál k csúcsnyit lép előre. Hány lépés után jut vissza a kiindulóponthoz? Hány kört tesz meg ezalatt? Hány csúcsot érint összesen?

1.5.5. Tétel. *Ha a z komplex szám rendje véges, és k egész szám, akkor*

$$\boxed{o(z^k) = \frac{o(z)}{(o(z), k)}.}$$

Ez a hatvány rendjének képlete.

Bizonyítás. Legyen $o(z) = n$, és írjuk fel a z hatványait sorban egy n-szög csúcsaira. Helyezzünk rá egy bolhát a $z^n = 1$-nél levő csúcsra. Amikor a z^k számot hatványozzuk, akkor mindig azokra a csúcsokra jutunk, ahol a bolha lesz, amikor k-asával ugrál (az első ugrás után a z^k-ban, azután a $(z^k)^2$-ben, és így tovább). A z^k rendje a hatványainak a száma, vagyis a bolha által érintett csúcsok száma, ami az előző feladat szerint $n/(n, k)$. □

A képlettel ellenőrizhetjük, hogy mivel $o(i) = 4$, azért valóban $o(i^2) = 4/(4, 2) = 2$, és $o(i^3) = 4/(4, 3) = 4$. Általában, ha

$$\varepsilon_k = \cos(2k\pi/n) + i \sin(2k\pi/n) = \varepsilon_1^k ,$$

akkor már láttuk, hogy ε_1-nek n különböző hatványa van, tehát a rendje n, és így a képlet szerint

$$o(\varepsilon_k) = o(\varepsilon_1^k) = \frac{n}{(n, k)} .$$

Ezt praktikusabban is megfogalmazhatjuk. Az ε_k képletében egyszerűsítsük le a k/n törtet. Ekkor elérhetjük, hogy k és n relatív prímek legyenek. Ilyenkor pedig a fenti képlet n-et ad eredményül. Ez az észrevétel igen hasznos konkrét számoláskor, feladatmegoldáskor, ezért egy külön állításba foglaljuk.

1.5.6. Állítás. *Egy $z \neq 0$ komplex szám rendje akkor és csak akkor véges, ha abszolút értéke 1, szöge pedig a 2π racionális többszöröse. Ha ez a racionális szám egyszerűsíthetetlen tört alakjában felírva p/q (ahol $q > 0$), akkor a z rendje q.*

1.5.7. Definíció. Az n rendű komplex számokat *primitív n-edik egységgyök*öknek nevezzük.

Ezek mind az n-edik egységgyökök között vannak, és a fenti képlet szerint pontosan azok az ε_k számok lesznek primitív n-edik egységgyökök, melyekre $(k, n) = 1$.

1.5.8. Tétel. *A primitív n-edik egységgyökök pontosan az*

$$\varepsilon_k = \cos(2k\pi/n) + i \sin(2k\pi/n)$$

alakú számok, ahol k és n relatív prímek, és $0 \leq k < n$. Számuk $\varphi(n)$, ahol φ a számelméletből ismert Euler-függvény (lásd B.0.5. Definíció). Egy komplex szám akkor és csak akkor n-edik primitív egységgyök, ha a hatványai pontosan az összes n-edik egységgyökök.

Bizonyítás. Csak az utolsó állítást nem láttuk be az eddigiek során. Ha ε primitív n-edik egységgyök, akkor a rendje n, ezért n különböző hatványa van. Ezek mind n-edik egységgyökök, és mivel abból is n darab van, mindet meg kell kapjuk. Megfordítva, ha ε hatványai pont az n-edik egységgyökök, akkor n különböző hatványa van, és így a rendje n. □

A rend fogalmának bevezetésével befejeztük a komplex számokkal való ismerkedést. Noha láttunk néhány geometriai alkalmazást, és a gyökvonás sem probléma többé, a harmadfokú egyenlettel kapcsolatos kérdéseket még nem tisztáztuk. Erre akkor kerül majd sor, amikor már eleget fogunk tudni polinomokról is. Mostantól kezdve *szám* alatt mindig komplex számot értünk.

Gyakorlatok, feladatok

1.5.5. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között:

(1) $x^3 = 1$.
(2) $x^4 = -4$.
(3) $x^8 = \sqrt{3} - i$.
(4) $x^n = -1$.

1.5.6. Gyakorlat. Mennyi a rendje az

$$1 + i, \quad (1 + i)/\sqrt{2}, \quad \cos(\sqrt{2}\pi) + i \sin(\sqrt{2}\pi), \quad \cos(336^\circ) + i \sin(336^\circ)$$

számoknak? Melyek ezek között az egységgyökök? Mely n-ekre lesznek ezek a számok n-edik egységgyökök? És primitív n-edik egységgyökök?

1.5.7. Gyakorlat. Mutassuk meg, hogy minden egységgyök pontosan egy n-re lesz primitív n-edik egységgyök, de végtelen sok n-re lesz n-edik egységgyök.

1.5.8. Gyakorlat. Mutassuk meg, hogy ha $n > 0$ egész, $\varepsilon \in \mathbb{C}$, és $\varepsilon^n = i$, akkor ε rendje véges, és néggyel osztható.

1.5.9. Gyakorlat. Ha ε primitív 512-edik egységgyök, mennyi lehet $o(-i\varepsilon)$?

1.5.10. Feladat. Hogyan függ össze egy komplex szám és az ellentettjének a rendje? (Először kis n számokra vizsgáljuk meg).

1.5.11. Gyakorlat. Szorozzuk össze a hatodik egységgyököket a negyedik egységgyökökkel az összes lehetséges módon. Hány különböző számot kapunk? Mi a helyzet, ha a hatodik és a hetedik egységgyököket szorozzuk össze?

1.5.12. Gyakorlat. Legyenek m és n pozitív egészek.

(1) Hány közös gyöke van az $x^n = 1$ és $x^m = 1$ egyenleteknek?
(2) Mutassuk meg, hogy egy n-edik és egy m-edik egységgyök szorzata nm-edik egységgyök.
(3) Bizonyítsuk be, hogy egy n-edik és egy m-edik primitív egységgyök szorzata akkor és csak akkor nm-edik primitív egységgyök, ha m és n relatív prímek.

1.5.13. Gyakorlat. Mennyi az n-edik egységgyökök összege, szorzata és négyzetösszege?

Az alábbi feladatokban használjuk fel a 2.2.17. Gyakorlatban bizonyított binomiális tételt.

1.5.14. Feladat. Hozzuk „zárt alakra” a következő összeget:

$$\binom{1867}{0} + \binom{1867}{4} + \binom{1867}{8} + \binom{1867}{12} + \dots .$$

1.5.15. Feladat. Fejezzük ki $\cos x$ és $\sin x$ segítségével $\sin 7x$-et. Általánosítsuk a kapott képletet.

1.6. A komplex számok precíz bevezetése

Bizonyára sok olvasónk hallott már Gödel nevezetes tételéről, amely nagyon durva fogalmazásban ezt állítja: nem lehet bebizonyítani, hogy a matematikában soha nem fog felbukkanni ellentmondás. (Ezt, sajnos, teljes szabatossággal be lehet bizonyítani.) Így teljes biztonságot nem érhetünk el a komplex számok bevezetésekor sem. De ha az igényeinket lejjebb adjuk, akkor sem lehetünk elégedettek a komplex számok eddig használt, szemléletes bevezetésével. Eleve zavaró például az, hogy még mielőtt összeadást és szorzást definiáltunk volna, már magában a komplex szám $a + bi$ definíciójában mindkettő szerepel. Márpedig a matematikában nem definiálhatunk egyetlen fogalmat sem Münchausen-módra, saját maga segítségével.

Érdemes tehát a komplex számok fogalmát egy fokkal precízebben bevezetni, mint ahogy eddig tettük, hogy ne adjon félreértésre alkalmat, hogy meggyőzhessük magunkat arról: ha a valós számokkal való számolás során nem lehet baj (ellentmondás), akkor a komplex számok használata esetében sem lesz. Természetesen mindez csak a szemléletesség rovására történhet. Ezért úgy kell ügyeskednünk, hogy a bevezetés végére érve az eddig szemléletesen használt fogalmakat, jelöléseket továbbra is ugyanúgy használhassuk, ne keletkezzenek felesleges bonyodalmak.

A komplex számok precíz bevezetése magasabb fokú matematikai érettséget igényel, mint amit a könyv eddigi részeiben feltételeztünk. Meggyőződésünk, hogy először a komplex számokkal (sőt, esetleg a polinomokkal) való számolás gyakorlati fogásait célszerű elsajátítani. Ezért *ezt a szakaszt teljes egészében apró betűs résznek érdemes tekinteni.* Csak a jobb olvashatóság kedvéért nem szerepel ebben a formában. A könyv első olvasásakor az olvasó nyugodtan átugorhatja, annál is inkább, mert a konstrukció igazán tanulságos mozzanatai később újra és újra megjelennek majd. Először a polinomok precíz bevezetésekor (2.3. Szakasz), később a hányadostest, vagy az egyszerű algebrai tesbővítés konstrukciójakor. Sőt, a faktorgyűrűk vizsgálatakor a komplex számok bevezetésére is egy alternatív, ugyancsak precíz módszert lelünk majd.

Abból indulunk ki, ahogy a komplex számok egyenlőségét definiáltuk. A komplex számokat a valós és képzetes részük egyértelműen meghatározza, és ezek tetszőleges valós számok lehetnek. Így az $a + bi$ komplex számra gondolva egy olyan matematikai objektumot kell keresnünk, amelyet az a és b számok (a sorrendre is tekintettel) egyértelműen meghatároznak. Ilyen objektum az (a, b) rendezett pár (de akinek jobban tetszik, gondolhat helyette a sík megfelelő pontjára is, és akkor egy füst alatt a komplex számok geometriai kapcsolatát is megkapja). Tehát a nem szemléletes, de jól kezelhető definíció a következő:

1.6.1. Definíció. Komplex számon egy $z = (a, b)$ rendezett párt értünk, ahol a és b valós számok. A $z = (a, b)$ komplex szám *valós része* a, *képzetes része* b.

A műveleteket is könnyen definiálhatjuk, ha suttyomban az (a, b) helyére odaképzeljük az $a + bi$-t, és így „átkódoljuk” az 1.3.1. Definíciót:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)(c, d) = (ac - bd, ad + bc)\,.$$

A komplex számok között most nincsenek ott a valós számok, hiszen azok nem rendezett párok. Az a valós számot $a + 0 \cdot i$-ként írtuk fel komplex számként, ehelyett az $(a, 0)$ párra

kell gondolnunk. Az ilyen párokkal ugyanúgy kell számolni, mint a valós számokkal, hiszen a fenti képletek szerint

$$(a, 0) + (c, 0) = (a + c, 0)$$
$$(a, 0)(c, 0) = (ac, 0)\,.$$

Másképp fogalmazva, a

$$\varphi : a \mapsto (a, 0)$$

leképezés (amely kölcsönösen egyértelmű a valós számok és az $(a, 0)$ alakú komplex számok között) tartja az összeadást és a szorzást is. Ezért az a számot *azonosítjuk* a neki megfelelő $(a, 0)$ komplex számmal. (Ennek az azonosításnak vannak precíz technikái, amivel a halmazelméletben ismerkedhetünk meg.)

Látszólag nincs ott az újsütetű komplex számok között az i sem. A szemléletes definíció szerint persze $i = 0 + 1 \cdot i$, és így bevezethetjük az

$$i = (0, 1)$$

jelölést. Ekkor a szorzás szabálya miatt

$$i^2 = (0, 1)(0, 1) = (-1, 0)\,,$$

amit a -1 számmal azonosítottunk. Magyarul $i^2 = -1$, immár precízen. Végül az összeadás és a szorzás szabálya szerint

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1)\,,$$

ezt a számot pedig éppen $a + bi$-vel azonosítottuk. Így a komplex számok tényleg az $a + bi$ alakú kifejezések, melyekkel a műveleteket úgy kell végezni, ahogyan már megszoktuk.

1.7. Összefoglaló

A modulo m maradékok $\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$ halmazán bevezettük a *modulo m összeadás és szorzás* fogalmát (1.1.1. Definíció), és felderítettük ezek alapvető tulajdonságait (1.1.2. Állítás). Megállapítottuk, hogy ezek nagyon hasonlítanak a számok közötti műveletek tulajdonságaira, valamint hogy *művelettartó* az a leképezés, amely minden egész számhoz a mod m maradékát rendeli (1.1.3. Állítás). A kivonást az ellentett hozzáadásaként, az osztást a reciprokkal (inverzzel) való szorzásként definiáltuk. Az ellentett mindig létezik, a reciprok azonban nem. Nyitva maradt a *nullosztómentesség* kérdése is: egy szorzat lehet-e nulla úgy, hogy egyik tényezője sem nulla. A maradékokkal való számolást felhasználtuk kombinatorikai és számelméleti feladatok megoldására.

Megbeszéltük a harmadfokú egyenlet megoldási ötletét, és ebből levezettük a Cardano-képletet, bár az még nem derült ki, hogy ez megadja-e az egyenlet összes megoldását. Konkrét példák alapján azt tapasztaltuk, hogy ha az egyenletnek csak egy valós gyöke van, akkor azt a képlet megadja, de három valós gyök esetén ezeket csak úgy tudjuk megkapni, ha hajlandók vagyunk formálisan számolni negatív számok négyzetgyökeivel.

Hogy a negatív számok négyzetgyökeivel való számolást precízzé tegyük, bevezettük a *komplex számokat,* mint $a + bi$ alakú formális kifejezéseket, ahol $i^2 = -1$. Felfedeztük az összeadás és a szorzás szabályait és tulajdonságait (1.3.1. Definíció, 1.3.2. Állítás), melyek szintén nagyon hasonlítanak a számok közötti műveletek tulajdonságaihoz. A valós számokat is ($a + 0 \cdot i$ alakú) komplex számnak képzeljük, és ezentúl „szám" alatt komplex számot értünk. Megmutattuk, hogy minden nem nulla komplex számmal lehet osztani (1.3.3. Állítás): a törtet a nevező *konjugáltjával* kell bővíteni. Ebből levezettük a nulloszthatóságmentességet is (1.3.4. Állítás). Kiterjesztettük az *abszolút érték* fogalmát komplex számokra (de leszögeztük, hogy komplex számok között nem értelmezünk egyenlőtlenségeket). Összefoglaltuk a konjugálás és az abszolút érték tulajdonságait (1.3.6. Állítás).

A komplex számokat a sík pontjaival, illetve az ezekbe az origóból mutató helyvektorokkal azonosítottuk. Ekkor a komplex számok összeadása a vektorösszeadásnak felel meg. Egy komplex szám abszolút értéke az origótól való távolsága, és emiatt teljesül a *háromszög-egyenlőtlenség* (1.4.2. Tétel). Definiáltuk nem nulla komplex szám *szögét,* és *trigonometrikus alakját.* Megállapítottuk, hogy komplex számok szorzásakor a hosszak összeszorzódnak, a szögek pedig (mod 2π) összeadódnak (1.4.3. Állítás). Így képletet kaptunk a gyors hatványozásra (pozitív és negatív egész kitevők esetében). Az a következmény, hogy egy komplex számmal való szorzás egy forgatva nyújtás, lehetővé teszi, hogy komplex számokat használjunk geometriai feladatok megoldásához.

Megállapítottuk, hogy egy nem nulla komplex számnak minden n pozitív egészre pontosan n darab n-edik gyöke van, amelyek egy origó középpontú szabályos sokszög csúcsaiban helyezkednek el. A *gyökvonást* trigonometrikus alakban célszerű elvégezni (1.5.2. Gyakorlat). Azokat az ε komplex számokat, amelyekre $\varepsilon^n = 1$ teljesül, *n-edik egységgyök*öknek neveztük. Ezek a $\cos(2k\pi/n) + i\sin(2k\pi/n)$ alakú számok, összesen n darab n-edik egységgyök van. Ha egy számnak ismerjük az egyik n-edik gyökét, akkor az összes n-edik gyökeit az n-edik egységgyökökkel való szorzással kapjuk (1.5.2. Tétel).

Egy $z \neq 0$ komplex szám $o(z)$ *rendje* a különböző hatványainak a száma. Ez vagy végtelen, ebben az esetben z bármely két egész kitevőjű hatványa különböző, vagy egy pozitív r szám, ebben az esetben z hatványai r szerint periodikusan ismétlődnek, vagyis

$$\boxed{\boxed{z^k = z^\ell \iff o(z) \mid k - \ell}}$$

(1.5.4. Tétel). Speciálisan z^n akkor és csak akkor 1, ha $o(z) \mid n$ (ezek a z szám „jó" kitevői). Egy z komplex szám rendje akkor és csak akkor véges, ha a szám egységgyök, vagyis ha hossza 1, szöge pedig a 2π racionális számszorosa. Ha ez a racionális szám p/q, és $(p, q) = 1$, akkor z rendje q (1.5.6. Állítás). Mindez a hatvány rendjének

$$\boxed{o(z^k) = \frac{o(z)}{(o(z), k)}}$$

képletéből következik (1.5.5. Tétel).

Egy szám *primitív* n-edik egységgyök, ha rendje n. Ezek a $\cos(2k\pi/n) + i\sin(2k\pi/n)$ alakú számok, ahol $(k, n) = 1$. Összesen $\varphi(n)$ darab primitív n-edik egységgyök van

(itt $\varphi(n)$ a számelméletből ismert Euler-függvény). Egy szám akkor és csak akkor n-edik primitív egységgyök, ha hatványai pontosan az összes n-edik egységgyökök (1.5.8. Tétel).

Végül mutattunk egy lehetséges módot a komplex számok precíz bevezetésére. Az $a + bi$-nek képzelt számot az (a, b) rendezett párként definiáltuk, és az ezek közötti műveleteket az 1.3.1. Definíció alapján adtuk meg (1.6.1. Definíció). Az a valós számot azonosítottuk az $(a, 0)$ komplex számmal, ezt azért tehettük meg, mert az összeadást és a szorzást mindkettővel „ugyanúgy" kell végezni. Ily módon a valós számok is komplex számokká váltak. Az $i = (0, 1)$ jelölést használva $(a, b) = a + bi$ adódott, és így precízzé tettük a komplex számok korábbi, szemléletes definícióját.

2. POLINOMOK

...de az a + b-t és a nullát, ami nem is nulla,
és az x-nek titokzatos hánytorgásait...

Fekete István: *Téli berek*

2.1. A polinom fogalma

Amikor közönséges egyenleteket kell megoldanunk, az ismeretlennel *formálisan* számolunk. Például az

$$\frac{x^2+x+1}{x+1}=x$$

egyenlet esetében nem próbálunk az x helyébe konkrét számokat helyettesíteni, hanem olyan átrendezést hajtunk végre, ami minden egyes x-re helyes. Így a fenti egyenletből $x+1$-gyel átszorozva

$$x^2+x+1=x^2+x$$

adódik. Ezt az átalakítást akkor is helyesnek érezzük, ha tudjuk, hogy ez utóbbi egyenletnek nincs megoldása (hiszen $1=0$-ra vezet), tehát semmilyen konkrét x számra nem teljesül egyik felírt egyenlőség sem.

Ahogy tehát a komplex számok bevezetése kapcsán megállapítottuk, hogy milyen szabályok szerint szabad számolni negatív számok négyzetgyökeivel, úgy érdemes most is megvizsgálni, hogy az „ismeretlen, meghatározatlan számokat" tartalmazó kifejezéseket hogyan kezelhetjük.

Miért van erre szükség? Hiszen az egyenletmegoldást már a középiskolában begyakoroltuk. A válasz ismét az, hogy szeretnénk sok problémára közös megoldási módszert találni. Ilyen például egy egyenlet megoldóképlete. Más esetben olyan, minél egyszerűbb kifejezést kell felírnunk, ami adott helyeken adott értékeket vesz fel (így kereshet például egy fizikus törvényt, szabályszerűséget a mérési eredményeihez). Ilyenkor ismernünk kell a felírandó kifejezések tulajdonságait. Az is előfordul, hogy meg szeretnénk bizonyosodni: egy bonyolult egyenletnek nincs már más megoldása, mint amiket megtaláltunk. Ehhez jól jönne egy olyan tétel, ami megmondja, hogy egy egyenletnek, az alakjától függően, maximum hány megoldása lehet.

De szükség lehet *negatív eredmények* bizonyítására is. A matematikában nagyon hasznos ismerni a *módszereink korlátait* is, hogy tudjuk: egy-egy probléma megoldásához kell-e új

módszert kifejleszteni. Fontos példa ilyen korlátra, hogy a legalább ötödfokú egyenletek esetében már nem létezik olyan általános megoldóképlet, amely a négy alapművelet és gyökvonás segítségével megadja az egyenlet gyökeit. Ennek a bizonyításához precízen tudnunk kell, mit is értünk egyenlet, gyökképlet alatt, és mik ezeknek a tulajdonságai.

A komplex számokhoz hasonlóan arra törekszünk, hogy az olvasó minél hamarabb el tudjon kezdeni számolni polinomokkal. Ezért a lehető legpraktikusabban vezetjük be ezt a fogalmat. A precíz bevezetés megtalálható a 2.3. Szakaszban.

Elsőként az olyan kifejezéseket vesszük górcső alá, amelyekben számokon kívül csak egy x „ismeretlen" szerepel, és csak három műveletet használhatunk: összeadást, kivonást és szorzást. A komplex számok bevezetésekor észrevettük, hogy minden i-t tartalmazó, a fenti három művelettel felírt kifejezés $a + bi$ alakra egyszerűsíthető. Középiskolás tapasztalatunk az, hogy a zárójelek felbontásával, és x hatványai szerinti rendezéssel az x-et tartalmazó, e három művelettel felírt kifejezések a következő alakra hozhatók:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \,,$$

ahol $a_0, \ldots, a_n$ számok, és $n \geq 0$ egész szám. Az ilyen kifejezéseket *polinomoknak* nevezzük. Az x a polinomban szereplő *határozatlan.* Az a_jx^j kifejezések a polinom *tagjai,* az a_i számok pedig a polinom *együtthatói.* Az a_0 a polinom *konstans tagja.*

Mivel formálisan számolunk, x-ről semmi mást nem tételezhetünk fel, csak azt, ami minden számra érvényes. Ezért $0 \cdot x$ természetesen nulla lesz, de a fenti képletben semmilyen más egyszerűsítési lehetőséget nem várhatunk. A $0 \cdot x^k$ tagot néha érdemes lesz kiírni, néha meg érdemes lesz elhagyni. Így tehát az $1 + x^2$ és az $1 + 0 \cdot x + x^2 + 0 \cdot x^3$ polinomokat egyenlőnek tekintjük. A legegyszerűbb, ha minden polinomba odaképzeljük a ki nem írt x-hatványokat is, nulla együtthatóval. Ekkor polinomok egyenlőségét a következőképpen definiálhatjuk.

2.1.1. Definíció. Két polinomot akkor és csak akkor tekintünk egyenlőnek, ha a megfelelő együtthatóik megegyeznek, vagyis ha minden $k \geq 0$ egészre az x^k együtthatója a két polinomban ugyanaz.

Ha a fenti f polinomban mindegyik a_i együttható nulla, akkor a *nullapolinomot* kapjuk (ez nem tévesztendő össze a 0 számmal, de mindkettőt 0 jelöli). Ha $f \neq 0$, akkor hagyjuk el a polinom jobboldaláról a nulla együtthatójú tagokat. Így

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$$

adódik, ahol $a_k \neq 0$. Ebben az esetben az k kitevő a polinom *foka,* az a_kx^k a polinom *főtagja,* az a_k szám pedig a polinom *főegyütthatója.* Egy polinom *normált,* ha főegyütthatója 1. Tehát csak a nem nulla polinomoknak értelmezzük a fokát. Az f polinom fokát $\mathrm{gr}(f)$-fel jelöljük (sok könyvben a $\deg(f)$ jelölést alkalmazzák). Egyenlő polinomoknak természetesen ugyanaz a foka (ha létezik). Az f helyett mindegyik jelölésben írhatunk $f(x)$-et is, ha fel akarjuk tüntetni, hogy x a határozatlan.

Ahhoz, hogy eldönthessük, tényleg minden vizsgált kifejezés a fenti alakra hozható-e, elegendő azt ellenőrizni, hogy a fenti alakú polinomokat összeadva, kivonva, és összeszorozva szintén ilyen alakú kifejezést kapunk. A komplex számok bevezetéséhez hasonlóan fontos lesz konkrétan kiszámolni az összeg és a szorzat képletét.

Két polinom összegének kiszámításához a kisebb fokú polinom végére írjunk nulla tagokat úgy, hogy a következő alakot kapjuk:

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\,, \qquad g = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n\,.$$

Tehát feltehető, hogy ugyanaz az n szám szerepel a két polinomban (de ekkor csak annyit tudunk, hogy polinomjaink foka legfeljebb n, tehát ilyenkor már nem tehetjük föl, hogy a két főegyüttható nem nulla). Ez a felírás azért hasznos, mert az összeadást könnyen elvégezhetjük:

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n\,.$$

Hasonló képlet adja két polinom különbségét is.

2.1.2. Állítás. *Két polinom összegének a foka legfeljebb akkora, mint a két polinom fokai közül a nagyobb (pontosabban a nem kisebb). Képletben:* $\mathrm{gr}(f+g) \le \max(\mathrm{gr}(f), \mathrm{gr}(g))$. *Ha a két polinom foka különböző, akkor egyenlőség áll.*

Bizonyítás. Az f és g felírásában (hacsak nem $f = g = 0$) feltehetjük, hogy a két főegyüttható egyike, mondjuk a_n, nem nulla. Ha $b_n = 0$, akkor az összeg főegyütthatója is a_n lesz. Ha azonban mindkét polinom foka n, akkor elképzelhető, hogy $a_n + b_n = 0$, sőt még az is, hogy az összegben minden együttható nullává válik (és ilyenkor az összegnek nincs is foka). □

2.1.1. Gyakorlat. Szorozzuk össze az $a_0+a_1x+a_2x^2$ és $b_0+b_1x+b_2x^2+b_3x^3$ polinomokat, bontsuk fel a zárójelet, rendezzük az eredményt x hatványai szerint, végül állapítsuk meg az eredmény fokát.

A polinomok szorzásakor a következő felírás lesz hasznos:

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\,, \qquad g = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m\,,$$

ahol $a_n \neq 0$ és $b_m \neq 0$. (Ha valamelyik tényező a nullapolinom, akkor a szorzat nyilván szintén nulla.) Szorozzuk össze ezt a két polinomot.

2.1.2. Gyakorlat. Mutassuk meg, hogy az $(a_1 + \cdots + a_n)(b_1 + \cdots + b_m)$ szorzat egyenlő az nm darab a_ib_j szám összegével.

A fenti észrevétel alapján az f és g szorzásánál a zárójelet úgy bonthatjuk ki, hogy az első összeg minden tagját megszorozzuk a második összeg minden tagjával, majd a kapott szorzatokat összeadjuk. Ezt az $(n+1)(m+1)$ tagú összeget szeretnénk x hatványai szerint rendezni. Egy x^k-os tag úgy tud keletkezni, hogy egy x^i-s és egy x^j-s tagot szorzunk össze, ahol $i + j = k$. Így az fg szorzatban x^k együtthatója

$$c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_{k-1}b_1 + a_kb_0\,. \tag{2.1.1}$$

Látszólag c_k egy $k+1$ tagú összeg, de valójában az összegnek lehet kevesebb tagja. Például ha $k = m + n$, akkor az $a_0 b_{n+m}$ tag nem fog szerepelni, mert b indexe csak nullától m-ig halad. Ezt a gondot azonban könnyen kiküszöbölhetjük, ha megállapodunk abban, hogy nullának tekintjük $b_{m+1}, b_{m+2}, \ldots$, és ugyanúgy $a_{n+1}, a_{n+2}, \ldots$ értékét (ahogy már a polinomok egyenlőségének 2.1.1. Definíciója előtt is tettük). Ezzel a fenti (2.1.1) képlet mindkét formája helyessé válik.

Az x^{n+m} tag együtthatója tehát egy $n + m + 1$ tagú összeg, de ennek csak egyetlen nem nulla tagja van: $a_n b_m$. Valóban, a tagok $a_i b_j$ alakúak, ahol $i + j = n + m$, és ha $i > n$, akkor $a_i = 0$, ha viszont $i < n$, akkor $j > m$, vagyis $b_j = 0$. Ez az egyetlen $a_n b_m$ tag viszont nem lesz nulla, mert egyik tényezője sem az. Ez bizonyítja a következő állítást.

2.1.3. Állítás. *Az fg szorzat főegyütthatója $a_n b_m$, foka $n+m$. Tehát nem nulla polinomok szorzásakor a fokok összeadódnak:* $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$. *Így a szorzatpolinom nem nulla, vagyis polinomok szorzására is érvényes a nullosztómentesség.*

A polinomokkal is a szokásos szabályok szerint számolhatunk. Foglaljuk össze bizonyítás nélkül ezeket a — remélhetőleg már ismerős — szabályokat.

2.1.4. Állítás. *Legyenek f, g, h tetszőleges polinomok.*

(1) $(f + g) + h = f + (g + h)$ *(az összeadás asszociatív).*
(2) $f + g = g + f$ *(az összeadás kommutatív).*
(3) $f + 0 = 0 + f = f$ *(azaz létezik nullelem).*
(4) *Minden f-nek van ellentettje, azaz olyan g, melyre $f + g = g + f = 0$. (Ilyen g lesz az a polinom, melynek együtthatói az f együtthatóinak ellentettjei.)*
(5) $(fg)h = f(gh)$ *(a szorzás asszociatív).*
(6) $fg = gf$ *(a szorzás kommutatív).*
(7) $f \cdot 1 = 1 \cdot f = f$ *(azaz létezik egységelem).*
(8) $(f + g)h = fh + gh$ *(disztributivitás).*

A (3) állításban szereplő 0 a nullapolinomot jelöli (és nem a 0 számot). Hasonlóképpen a (7) állításban szereplő 1 jel polinom, és nem szám: az a polinom, amelynek minden együtthatója nulla, kivéve a konstans tagot, ami 1. Általában tetszőleges c számot polinomnak is tekinthetünk. Ezek a *konstans polinomok*, azaz a nulladfokú polinomok és a nullapolinom. A konstans polinomokat ugyanúgy kell összeadni és szorozni, mint a megfelelő számokat.

Mivel minden polinomnak létezik ellentettje, a kivonás is korlátlanul elvégezhető (mint az ellentett hozzáadása). Korábban láttuk, hogy az osztást (a maradékokkal való számolásnál is, a komplex számoknál is) a reciprokképzésre, vagyis az inverz elemmel való szorzásra vezethetjük vissza. Így van ez a polinomoknál is, de csak nagyon kevés polinomnak van reciproka.

2.1.5. Állítás. *Az f polinomnak akkor és csak akkor van inverze (reciproka) a polinomok között, ha f nem nulla konstans polinom.*

Bizonyítás. Ha $c \neq 0$ konstans polinom, akkor inverze az $1/c$ konstans polinom (és így minden polinom eloszthető vele: az együtthatóit kell c-vel elosztani). Tegyük most fel, hogy az f polinomnak van inverze. Ez azt jelenti, hogy létezik olyan g polinom, hogy $fg = 1$. Így egyik tényező sem nulla, vagyis képezhetjük a szereplő polinomok fokát. Mivel szorzásnál a fokok összeadódnak, azt kapjuk, hogy

$$\mathrm{gr}(f) + \mathrm{gr}(g) = \mathrm{gr}(fg) = \mathrm{gr}(1) = 0\,.$$

Ezért f és g foka is nulla kell, hogy legyen, vagyis f csak konstans polinom lehet. □

Mielőtt továbblépnénk, bevezetünk egy jelölést, amit sokszor használunk majd a későbbiekben. Egy soktagú összeg jelölésére eddig a ... szimbólumot használtuk, például $a_1 + a_2 + \cdots + a_n$ jelentette azt, hogy az a_i számokat össze kell adni, miközben az i index 1-től n-ig fut. Ezzel a jelöléssel azonban több probléma is lehet. Ha az a_i egy bonyolult kifejezés, akkor esetleg kényelmetlen, vagy áttekinthetetlen leírni több tagot is (ahogy az imént három konkrét tagot is leírtunk: a_1-et, a_2-t és a_n-et). Esetleg nem is könnyű kitalálni, mire gondolhat az, aki mondjuk az $a_1 + a_3 + \cdots + a_n$ összeget írta le. Vajon itt a páratlan indexű a_i számokat kell összeadni? E problémák áthidalására a következő jelölés szolgál.

2.1.6. Definíció. A

$$\sum_{j=1}^{n} a_j$$

úgynevezett *szumma jelölés* azt jelenti, hogy a j változó 1-től n-ig fut, és minden értékére össze kell adni a szumma jel jobboldalán álló a_j kifejezést. A

$$\prod_{j=1}^{n} a_j$$

produktum jelölés a szumma jelöléstől abban különbözik, hogy itt az a_j kifejezéseket össze kell szorozni.

Vagyis a fenti definícióban az $a_1 + a_2 + \cdots + a_n$ összeg, illetve az $a_1 a_2 \ldots a_n$ szorzat tömör jelölése szerepel. Sokszor előfordul, hogy a szummázás nem $i = 1$-től n-ig, hanem $i = m$-től n-ig megy. Sőt, azt is megtehetjük, hogy a szumma jel alá egy feltételt írunk, és akkor a szummázást azokra az indexekre kell végrehajtani, amelyekre ez a feltétel teljesül. Például

$$\sum_{p\,<\,1000,\ p\ \text{prím}} p^2$$

az 1000-nél kisebb prímszámok négyzetösszege. Az új jelöléssel a szorzatpolinomnak a (2.1.1) képletben szereplő általános együtthatóját többféleképpen is felírhatjuk:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j$$

(a második szummában hallgatólagosan azt feltételeztük, hogy i és j nemnegatív egészek).

Ebben a szakaszban megismerkedtünk az egyhatározatlanú polinomok fogalmával, és néhány alapvető tulajdonságukkal. Sokszor előfordul, hogy több ismeretlenünk is van (és esetleg több egyenlet). Célszerű lenne tehát polinomnak tekinteni mondjuk az

$$x^2y^2 - 6xy^4 + \pi x - ix^2 + y + 2$$

kifejezést is. Az eddigiekhez hasonló módon definiálhatnánk a *többhatározatlanú* polinomok fogalmát, és levezethetnénk a műveleti szabályokat. Azonban a képleteink egyre bonyolultabbak lennének, és különben sem hasznos dolog sokszor végigcsinálni lényegében ugyanazt. Ezért más utat fogunk keresni.

Ezt az új utat a következő probléma megoldása jelöli ki: nullosztómentes-e a szorzás a többhatározatlanú polinomok között? Elvileg előfordulhatna, hogy amikor a szorzást elvégezzük, akkor a zárójel felbontása után keletkező összes tag kipotyog. Láttuk, hogy az egyhatározatlanú polinomok között ez nem történhet meg, az oka az volt, hogy ha a polinomok legmagasabb fokú tagjai a_nx^n és b_mx^m, akkor csak egyetlen x^{n+m}-es tag keletkezik a szorzásnál, és ezért az biztosan nem fog kiesni.

Többhatározatlanú polinomnál azonban vigyáznunk kell: a fenti polinomban x^2y^2-et vagy xy^4-t tekintsük-e magasabb fokú tagnak? Úgy érdemes eljárni, hogy kijelöljük az egyik határozatlant, mondjuk az x-et, és a polinomot az x hatványai szerint rendezzük:

$$(y^2 - i)x^2 + (-6y^4 + \pi)x + (y + 2)\,.$$

Az együtthatók most már nem számok, hanem y polinomjai, de ez nem gond, hiszen *számolni* azokkal is tudunk! Beszélhetünk főegyütthatóról is, ez most $y^2 - i$. A nullosztómentességhez az kell, hogy a két összeszorzott polinom főegyütthatójának szorzata ne legyen nulla, és ez igaz, mert y polinomjairól már beláttuk a nullosztómentességet.

A többhatározatlanú polinomok vizsgálatához tehát arra van szükség, hogy a polinomokat általánosan vezessük be: az együtthatókról ne tegyük fel, hogy számok, hanem csak azt, hogy *a szokásos szabályok szerint lehet velük számolni*. Ez más területen is kamatozna, például számelméleti feladatoknál, mert itt néha olyan egyenleteket kell megoldani, ahol az együtthatókkal modulo m kell számolni. Az is elképzelhető, hogy egy-egy alkalmazásban csak az egész, vagy csak a racionális együtthatójú polinomokat célszerű megengednünk. E problémák megoldása érdekében a most következő két szakaszban (2.2 és 2.3) egy kitérőt teszünk.

Az olvasó bátran megteheti, hogy ezt a kitérőt egyelőre átugorja, és a polinomokat továbbra is úgy tekinti, hogy az együtthatóik számok. Ha így tesz, akkor ezzel a szemlélettel megértheti a 2.4. Szakaszban leírtak lényegét, de ha a többhatározatlanú polinom fenti, szemléletes „definícióját" elfogadja, akkor a polinomokról szóló további anyag nagy részét is. Ezzel a rutinnal felvértezve a következő két szakaszhoz való visszatérés sem okozhat már gondot. Ekkor azonban tegye meg, hogy még egyszer végigszalad a polinomokról szóló anyagrészeken, és meggyőződik arról, hogy az ott írottak tetszőleges (tehát nem feltétlenül szám-együtthatós) polinomokra is ugyanúgy érvényesek.

Gyakorlatok, feladatok

2.1.3. Gyakorlat. Végezzük el az alábbi műveleteket a komplex együtthatós polinomok körében, és állapítsuk meg az eredmény fokát.
a) $(x^3 + 3x^2 + 2) - (x^3 + 3x - 4)$.
b) $(x^2 + ix + 3)(x^2 + i)$.

2.1.4. Gyakorlat. Mivel egyenlő az $(a_1 + b_1) \dots (a_n + b_n)$ szorzat? (Először $n = 3$-ra fejtsük ki.) Mi történik, ha sok tényezőt szorzunk össze, amelyek mindegyike soktagú összeg?

2.1.5. Gyakorlat. Igazoljuk a

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij}$$

azonosságot.

2.2. A szokásos számolási szabályok

Az előző szakaszban megállapítottuk, hogy a polinomokat úgy lenne érdemes bevezetni, hogy az együtthatóikról semmi mást nem teszünk föl, mint hogy azokkal a szokásos szabályok szerint számolni lehet. Ezeket a „szokásos" szabályokat már három ízben megfogalmaztuk: az 1.1.2, 1.3.2 és 2.1.4. Állításokban. Kézenfekvő tehát most már *általában* megfogalmazni őket, hogy ne kelljen még ötödször, hatodszor, hetedszer leírni ugyanazt, hanem egy szóval hivatkozhassunk rájuk. Ez a szakasz az új elnevezések bevezetését, felsorolását tartalmazza.

Adott tehát egy R halmaz, amin műveleteket (összeadást, szorzást) értelmezünk valamilyen módon. Egy kétváltozós $*$ művelet tehát semmi egyebet nem jelent, mint hogy R bármely két a és b elemét „össze tudjuk műveletezni" (összeadni, összeszorozni), és az $a * b$ eredmény szintén az R halmaznak egy eleme lesz. Vagyis egy kétváltozós művelet egy tetszőleges kétváltozós függvény az R halmazon, amely szintén az R halmazba képez.

Nagyon vigyázzunk arra, amikor egy műveletet megadunk, hogy azt tényleg *minden elempárra, egyértelműen* definiáljuk. Ezt mindig elsőnek érdemes ellenőrizni. Például a kivonás *nem művelet* a pozitív számok halmazán, hiszen a $3 - 5$ eredménye nincs benne ebben a halmazban. Viszont művelet lesz az egész számok halmazán, hiszen bármely két egész szám különbsége is egész szám

Most áttekintjük a műveletek már ismerős tulajdonságait.

2.2.1. Definíció. Legyen $*$ kétváltozós művelet az R halmazon. Azt mondjuk, hogy ez

(1) *asszociatív*, ha tetszőleges $x, y, z \in R$ esetén $(x * y) * z = x * (y * z)$;
(2) *kommutatív*, ha tetszőleges $x, y \in R$ esetén $x * y = y * x$.

Az asszociativitás azt jelenti, hogy a háromtényezős szorzatokat zárójelek nélkül írhatjuk fel (de a sorrendre ügyelnünk kell). Ebből már (nem könnyen, de) be lehet bizonyítani, hogy a több tényezős szorzatok felírásakor sem kell zárójeleket használni. Az olvasó esetleg meg is próbálkozhat a bizonyítással.

2.2.1. Feladat. Mutassuk meg, hogy ha $*$ asszociatív művelet, akkor az $a_1 * a_2 * \cdots * a_n$ szorzatot akárhogyan is zárójelezzük, az eredmény mindig ugyanaz lesz.

Asszociatív műveletre az egyik legfontosabb, eddig még nem szerepelt példa az, amikor függvényeket helyettesítünk egymásba. Legyen X tetszőleges halmaz, és R az összes X-et X-be képző (egyváltozós) függvények halmaza. Ha $f, g \in R$, akkor $f \circ g$ azt a függvényt jelöli, amikor f-be g-t helyettesítünk, vagyis először g-t, majd f-et alkalmazzuk. Képlettel kifejezve

$$(f \circ g)(x) = f\big(g(x)\big)$$

tetszőleges $x \in X$ esetén. Az $f \circ g$ neve az f és g *kompozíciója.* Az analízisben néha ehelyett *összetett függvény* képzéséről beszélnek.

Ez a művelet általában nem kommutatív. Nem mindegy, hogy a csirkét előbb megkopasztjuk, és azután megsütjük, vagy előbb megsütjük, és azután megkopasztjuk. A kompozíció művelete azonban mindig asszociatív.

2.2.2. Gyakorlat. Mutassuk meg, hogy a kompozíció művelete asszociatív. Adjunk példát két geometriai transzformációra, ami azt mutatja, hogy a kompozíció nem kommutatív.

A kommutativitás azt jelenti, hogy a soktényezős szorzatok esetében is mindegy a tényezők sorrendje.

2.2.3. Feladat. Mutassuk meg, hogy ha $*$ asszociatív és kommutatív művelet, akkor az $a_1 * a_2 * \cdots * a_n$ szorzat tényezőit bármilyen sorrendben is írjuk fel, az eredmény mindig ugyanaz lesz.

Az összeadás „szokásos tulajdonságai” között mindig felsoroltuk azt, hogy van egy „nulla” nevű elem, amihez bármely x számot hozzáadva ezt az x számot kapjuk eredményül. A szorzásnál ugyanezt a tulajdonságot emlegettük, csak ott egységelemről beszéltünk nullelem helyett. Általános művelet esetén (ami lehet összeadás, szorzás, vagy egész más is), célszerű egy új nevet bevezetni, amit mindig használhatunk.

2.2.2. Definíció. Legyen $*$ kétváltozós művelet az R halmazon. Azt mondjuk, hogy az $e \in R$ *neutrális* (=semleges) *elem,* ha tetszőleges $x \in R$ esetén $e * x = x * e = x$. Ha a művelet jele $+$, akkor általában *nullelemről* beszélünk, és a 0 jelet használjuk. Ha viszont a művelet szorzás (amit a leggyakrabban egyszerűen egymás mellé írással jelülünk), akkor a neutrális elemet *egységelemnek* hívjuk, és 1-gyel jelöljük.

2.2.4. Gyakorlat. Melyik függvény lesz a kompozícióra nézve neutrális elem?

Nemkommutatív művelet esetében szokás *bal oldali neutrális elemről* is beszélni, ha csak azt követeljük meg, hogy $e*x = x$ teljesüljön minden x-re. Hasonlóan *e jobb oldali neutrális elem,* ha minden x-re $x*e = x$. Ebben a könyvben vizsgálunk ugyan fontos nemkommutatív műveleteket, de az egyoldali neutrális elem csak ritkán fog szerepet játszani.

2.2.5. Feladat. Mutassuk meg, hogy tetszőleges műveletre nézve legfeljebb egy neutrális elem lehet.

Több konkrét példán is láttuk már, hogy a kivonást az ellentett hozzáadásaként, az osztást pedig a reciprokkal való szorzásként definiálhatjuk. Ezért most, amikor ezeket a fogalmakat általában vezetjük be, elsőnek az ellentett, illetve a reciprok képzésével kell foglalkoznunk. Ez a két név valójában ugyanazt a fogalmat takarja (csak a művelet más).

2.2.3. Definíció. Legyen e neutrális elem a $*$ műveletre nézve. Ha $u*v = e$, akkor azt mondjuk, hogy u *balinverze* v-nek, v pedig *jobbinverze* u-nak. Ha $v*u = e$ is teljesül, akkor azt mondjuk, hogy u és v egymás *inverzei.* Ha egy elemnek van kétoldali inverze, akkor *invertálhatónak* nevezzük. Ha a művelet a $+$, akkor inverz helyett *ellentettről* beszélünk. Ilyenkor a $v = -u$ jelölést alkalmazzuk. Ha a művelet jele a szorzás (vagy egymás mellé írás), akkor u inverzét u^{-1}-gyel jelöljük.

2.2.6. Feladat. Legyen $*$ asszociatív, de nem feltétlenül kommutatív művelet, melynek van neutrális eleme.

(1) Mutassuk meg, hogy ha egy u elemnek van balinverze is és jobbinverze is, akkor ez a kettő egyenlő (és így u invertálható). Speciálisan ha egy elemnek van kétoldali inverze, akkor ez az egyetlen balinverze és az egyetlen jobbinverze, vagyis *az inverz egyértelmű.*
(2) Ha az u és v elemek is invertálhatók, akkor mi lesz az $u*v$ inverze?

Az összeadásra vonatkozó „szokásos számolási szabályokat” úgy foglaltuk össze, hogy a most definiált tulajdonságokból többet is felhasználtunk. Érdemes külön nevet is adni a tulajdonságok ilyen csoportjainak.

2.2.4. Definíció. Ha egy nem üres halmazon értelmezett egy asszociatív művelet, akkor *félcsoportról* beszélünk.

Ha egy félcsoportban minden elemmel lehet osztani, akkor azt csoportnak nevezzük. Ehhez persze elegendő, ha minden elemnek van inverze.

2.2.5. Definíció. Egy G nem üres halmaz *csoport*, ha értelmezett rajta egy $*$ művelet a következő tulajdonságokkal.

(1) A $*$ művelet asszociatív.
(2) Van neutrális eleme.
(3) G minden elemének van inverze.

Mint láttuk, a neutrális elem egyértelmű, és az inverz létezése természetesen erre a neutrális elemre vonatkozik. Az inverzképzést szokásosabb külön (egyváltozós) műveletként bevezetni. Ennek előnyéről szólunk majd a 8.4. Szakaszban. Most az a fontos számunkra, hogy a fent megfogalmazott definíció a lehető legegyszerűbb legyen. Ha inverzről esik szó, akkor ebbe ezentúl automatikusan beleértjük, hogy létezik a megfelelő neutrális elem is.

A csoport definíciójában tehát nem tesszük föl, hogy a művelet kommutatív. Ha mégis az, akkor az ilyen csoportot *kommutatív csoportnak,* vagy *Abel-csoportnak* nevezzük. Nagyon gyakori, hogy Abel-csoportok esetében a műveletet $+$ jelöli. Ilyenkor tehát v ellentettje $-v$, és definiálhatjuk a *kivonást* az $u - v = u + (-v)$ képlettel.

Ha a csoport nem kommutatív, akkor viszont inkább egymás mellé írással jelöljük a műveletet. Ilyenkor osztásról nem lesz szó, mert u és v hányadosát kétféleképpen is definiálhatnánk: $v^{-1}u$-nak is és uv^{-1}-nek is. (Néha beszélnek ennek megfelelően balosztásról és jobbosztásról.)

A bal- és jobboldali osztás közötti elvi különbséget érdekesen illusztrálja az osztás általános iskolában tanított kétféle fogalma. Ha egy étteremben 10 asztal van, és mindegyiknél négy vendég ül, akkor az étteremben $4 \cdot 10 = 40$ vendég van. Természetesen $4 \cdot 10 = 10 \cdot 4$, hiszen a szorzás az egész számok között kommutatív. De e két szorzatnak mégis más a *jelentése,* ha megállapodunk, hogy az első tényező mindig a csoportok létszámát, a második pedig a csoportok számát jelenti. Ha a kérdés az (40 vendég esetén), hogy „ha minden asztalnál négyen ülnek, hány asztal van", akkor ezt a feladatot *bennfoglalásnak* nevezik. Ha viszont az a kérdés, hogy „ha tíz asztal van, hányan ülnek egy asztalnál", akkor *részekre osztás*nak. Az első esetben balosztásról van szó (4-gyel), a másodikban jobbosztásról (10-zel). Persze a kommutativitás miatt ugyanannak a két számnak a bal- és a jobboldali hányadosa ugyanaz lesz, tehát számolnunk ugyanúgy kell, de a számolás értelme más a két esetben. Nemkommutatív műveletnél az eredmény is lehet más.

Most röviden összefoglaljuk, hogy az eddig megismert konkrét műveletek milyen tulajdonságúak, de már az újonnan született nyelvünkön. Azt javasoljuk, hogy az olvasó ellenőrizze az alábbi állításokat.

2.2.6. Állítás. *Kommutatív csoportot alkotnak:*

(1) *A komplex számok az összeadásra:* $\mathbb{C}^+$.
(2) *A nem nulla komplex számok a szorzásra:* $\mathbb{C}^\times$.
(3) *A valós számok az összeadásra:* $\mathbb{R}^+$.
(4) *A nem nulla valós számok a szorzásra:* $\mathbb{R}^\times$.
(5) *A racionális számok az összeadásra:* $\mathbb{Q}^+$.
(6) *A nem nulla racionális számok a szorzásra:* $\mathbb{Q}^\times$.
(7) *Az egész számok az összeadásra:* $\mathbb{Z}^+$.
(8) *A komplex együtthatós polinomok az összeadásra:* $\mathbb{C}[x]^+$.
(9) *A* $\{0, 1, \ldots, m-1\}$ *halmaz a modulo* m *összeadásra:* $\mathbb{Z}_m^+$.
(10) *Az* $\{1, 2, 3, 4\}$ *halmaz a modulo* 5 *szorzásra:* $\mathbb{Z}_5^\times$ *(ezt a jelölést majd később magyarázzuk meg).*

A felsorolt csoportok között persze összefüggés van. Ha tudjuk, hogy hogyan kell összeadni a komplex számokat, akkor ebből megkaphatjuk, hogy hogyan kell összeadni a valósakat, a racionálisakat, az egészeket, hiszen ezek mind részhalmazai a komplex számoknak.

2.2.7. Definíció. Legyen G egy csoport. Ha H részhalmaza G-nek, amely maga is csoport a G-beli műveletre nézve, akkor azt mondjuk, hogy H *részcsoportja* G-nek. Ezt úgy jelöljük, hogy $H \leq G$.

Például $\mathbb{Z}^+ \leq \mathbb{Q}^+ \leq \mathbb{R}^+ \leq \mathbb{C}^+$ és $\mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$. Ugyanakkor $\mathbb{Q}^\times$ nem részcsoportja $\mathbb{C}^+$-nak, mert más a művelet. Ugyanúgy $\mathbb{Z}_5^+$ nem részcsoportja $\mathbb{Z}^+$-nak, mert itt is más a művelet: $2+4=6$, de $2+_5 4=1$. (Erre különösen kell figyelnünk akkor, ha az egyszerűbb jelölés kedvéért $+_5$ helyett $+$-t írunk).

Általában hogyan lehet ellenőrizni, hogy egy részhalmaz részcsoport-e? A legelső kérdés, hogy egyáltalán *el tudjuk-e végezni a műveletet a H halmazon belül.* Ha például $G=\mathbb{R}^+$, és H a -10 és 10 közötti számokból áll, akkor ebben a H halmazban nem is tudjuk elvégezni az összeadást, az *kivezet belőle:* például $8, 9 \in H$, de $8+9 \notin H$. Elsőként tehát azt kell ellenőriznünk, hogy a H részhalmaz *zárt-e* G műveletére.

Az asszociativitást nem kell megvizsgálnunk, az automatikusan öröklődik, hiszen a bővebb G halmazon már tudjuk, hogy teljesül. A következő kérdés, hogy van-e H-nak neutrális eleme, és hogy elvégezhető-e benne az inverzképzés. Be lehet látni, hogy egy részcsoport neutrális eleme ugyanaz kell, hogy legyen, mint az eredeti csoporté, és így az inverzet is ugyanúgy kell kiszámítani. Az alábbi állításban összefoglaljuk, hogyan célszerű ellenőrizni, hogy egy részhalmaz részcsoport-e.

2.2.7. Feladat. Mutassuk meg, hogy ha G csoport egy $*$ műveletre, akkor egy $H \subseteq G$ részhalmaz akkor és csak akkor részcsoport, ha

(1) H zárt a $*$ műveletre, azaz $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$;
(2) H tartalmazza G neutrális elemét;
(3) H zárt a G-beli inverzképzésre, azaz ha $h \in H$, akkor $h^{-1} \in H$.

Igazoljuk azt is, hogy tetszőleges H részcsoport neutrális eleme ugyanaz, mint G neutrális eleme.

Következő célunk a „többszörös”, illetve „hatvány” fogalmának általánosítása. Mindkét esetben arról van szó, hogy egy műveletet (a többszörös esetében az összeadást, hatványozás esetében a szorzást) sokszor végzünk el.

2.2.8. Definíció. Legyen $*$ asszociatív művelet az R halmazon, és $a \in R$. Ekkor tetszőleges n pozitív egészre legyen

$$a^n = a * a * \ldots * a \quad (n \text{ tényező}).$$

Ha $*$-ra nézve van egy e neutrális elem, akkor legyen $a^0 = e$. Végül ha a invertálható, és inverze b, akkor legyen

$$a^{-n} = b^n .$$

Ezek az a elem egész kitevőjű *hatványai*. Ha a műveletet $+$ jelöli, akkor hatvány helyett *többszörösről* beszélünk, és az *na* írásmódot alkalmazzuk.

Most áttekintjük a hatványozás ismert azonosságait.

2.2.8. Gyakorlat. Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Mutassuk meg a következőket.

(1) a^{-n} az a^n inverze.
(2) $a^m a^n = a^{m+n}$.
(3) $(a^m)^n = a^{mn}$.
(4) Ha a és b *felcserélhető,* azaz $ab = ba$, akkor $(ab)^n = a^n b^n$.

A „szokásos" számolási szabályokban egyszerre szerepelt összeadás és szorzás is, ezeket a disztributivitás kapcsolta össze. Az ilyen struktúrát gyűrűnek nevezzük.

2.2.9. Definíció. Az R *gyűrű*, ha az R halmazon értelmezett egy összeadásnak nevezett $+$ jelű művelet is, és egy szorzásnak nevezett, általában egymás mellé írással jelölt művelet is, a következő tulajdonságokkal.

(1) R az összeadásra nézve Abel-csoport.
(2) R a szorzásra nézve félcsoport (azaz a szorzás asszociatív).
(3) Érvényes a *disztributivitás:* tetszőleges $x, y, z \in R$ esetén

$$(x + y)z = xz + yz \qquad \text{és} \qquad z(x + y) = zx + zy.$$

A gyűrűbeli szorzást nem definiáltuk kommutatívnak (ezért kellett két disztributív azonosságot is felírni), és azt sem tettük fel, hogy van rá nézve egységelem. Ha a szorzás kommutatív, akkor *kommutatív gyűrűről,* ha van egységelem, akkor *egységelemes gyűrűről* beszélünk.

Az összeadásra kapott csoportot az R *additív csoportjának* nevezzük, és R^+-szal jelöljük. Egységelemes gyűrűben van értelme annak, hogy egy elem invertálható-e vagy sem. A 2.2.6. Feladatból kapjuk, hogy az R invertálható elemei csoportot alkotnak az R-beli szorzásra, melynek egységeleme a gyűrű egységelemével egyenlő. Ez az R *multiplikatív csoportja*, jele $R^\times$.

Azt a gyűrűt, aminek a nulla az egyetlen eleme, *nullgyűrűnek* nevezzük. Ezt nem tekintjük egységelemes gyűrűnek. A többi egységelemes gyűrű esetében az egységelem különbözik a nullelemtől, és ilyenkor a multiplikatív csoportban nem lehet benne a nulla (más szóval a nullával soha nem lehet osztani). Mindez a következő állításból következik.

2.2.9. Feladat. Mutassuk meg, hogy egy gyűrűben a nullával való szorzás mindig nullát ad eredményül, és így egy invertálható elem (speciálisan az egységelem) nem lehet nullával egyenlő. Igazoljuk azt is, hogy tetszőleges r és s elemekre $r(-s) = (-r)s = -(rs)$.

Az olyan kommutatív, egységelemes gyűrűket, amelyben *minden nem nulla elemmel lehet osztani,* testnek nevezzük. (A nullgyűrű tehát nem test, mert nem is egységelemes.)

2.2.10. Definíció. Ha egy gyűrű nem nulla elemei csoportot alkotnak a szorzásra, akkor a gyűrűt *ferdetestnek* hívjuk. Ha egy ferdetest kommutatív, akkor *testről* beszélünk.

2.2.11. Állítás. *Kommutatív, egységelemes gyűrűt alkotnak:*

(1) *A komplex számok:* $\mathbb{C}$.
(2) *A valós számok:* $\mathbb{R}$.
(3) *A racionális számok:* $\mathbb{Q}$.
(4) *Az egész számok:* $\mathbb{Z}$.
(5) *A komplex együtthatós polinomok:* $\mathbb{C}[x]$.
(6) *A* $\{0, 1, \ldots, m-1\}$ *halmaz a modulo* m *összeadásra és szorzásra:* $\mathbb{Z}_m$.

A felsoroltak közül $\mathbb{C}$, $\mathbb{R}$ *és* $\mathbb{Q}$ *testek is.*

Azt, hogy mikor lesz $\mathbb{Z}_m$ test, nemsokára megvizsgáljuk. A fenti példákban, a csoportokhoz hasonlóan, többször előfordul, hogy az egyik gyűrű részhalmaza egy másiknak.

2.2.12. Definíció. Legyen R egy gyűrű. Ha S részhalmaza R-nek, amely maga is gyűrű az R-beli műveletekre nézve, akkor azt mondjuk, hogy S *részgyűrűje* R-nek. Ezt úgy jelöljük, hogy $S \leq R$. Ha R és S testek, akkor *résztestről* beszélünk. Ilyenkor azt is mondjuk, hogy az R test *bővítése* az S testnek.

Például $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ résztestek, és $\mathbb{Z}$ részgyűrűje $\mathbb{Q}$-nak. Azt, hogy egy részhalmaz részgyűrű illetve résztest-e, szintén a műveletekre való zártság vizsgálatával ellenőrizhetjük, a műveleti azonosságokkal (asszociativitás, disztributivitás) nem kell foglalkoznunk.

2.2.10. Feladat. Mutassuk meg, hogy ha R gyűrű, akkor egy $S \subseteq R$ részhalmaz akkor és csak akkor részgyűrű, ha

(1) S zárt az R összeadására és szorzására, azaz $r_1, r_2 \in S$ esetén $r_1 + r_2$ és $r_1 r_2 \in S$;
(2) S tartalmazza R nullelemét;
(3) S zárt az R-beli ellentettképzésre, azaz ha $r \in S$, akkor $-r \in S$.

Ha R test, akkor az S részgyűrű pontosan akkor résztest, ha

(4) S tartalmazza R egységelemét;
(5) S zárt az R-beli inverzképzésre, azaz ha $0 \neq r \in S$, akkor $r^{-1} \in S$.

Tetszőleges S részgyűrű nulleleme ugyanaz, mint R nulleleme, és ha R test, akkor tetszőleges S résztest egységeleme ugyanaz, mint R egységeleme.

Megjegyezzük, hogy általában egy részgyűrű egységeleme különbözhet a gyűrű egységelemétől (lásd a 2.4.16. Feladatot).

Az eddig vizsgált konkrét gyűrűk többségében fontos észrevétel volt, hogy egy szorzat csak úgy lehet nulla, ha valamelyik tényezője nulla. Ilyen például $\mathbb{C}$ összes részgyűrűje, de a $\mathbb{Z}_6$ gyűrű nem ilyen, mert itt a nem nulla 2 és 3 elemek szorzata nulla lesz.

2.2.13. Definíció. Ha egy R gyűrűben $uv = 0$, de sem u sem v nem nulla, akkor azt mondjuk, hogy u baloldali, v pedig jobboldali *nullosztó*. Az R *nullosztómentes,* ha nincsen benne nullosztó, vagyis $uv = 0$-ból $u = 0$ vagy $v = 0$ következik.

Egy u elem tehát akkor baloldali nullosztó, ha nem nulla, és van olyan v nem nulla elem, amelyre $uv = 0$ teljesül.

2.2.11. Gyakorlat. Mutassuk meg, hogy ha egy R gyűrű egy u eleme nem baloldali nullosztó, akkor szabad vele balról egyszerűsíteni, azaz tetszőleges $r, s \in R$ esetén $ur = us$-ből $r = s$ következik. Igaz-e az állítás megfordítása?

Ezzel elérkeztünk ahhoz a ponthoz, hogy beláthatjuk első absztrakt algebrai tételünket.

2.2.14. Tétel. *Minden ferdetest nullosztómentes.*

Bizonyítás. Most is, a későbbiekben is, gyakran fogunk olyan bizonyításokkal találkozni, ahol az „aprómunkát" már korábban elvégeztük, és csak ellenőrizni kell egy korábbi bizonyításról, hogy az ott szereplő gondolatok valójában az általánosabb állítást is kiadják. Lapozzuk fel annak bizonyítását, hogy a komplex számok között érvényes a nullosztómentesség (1.3.4. Következmény). Vegyük észre, hogy az ottani gondolatmenet szó szerint elmondható a mostani körülmények között is, még azt sem használtuk fel, hogy a szorzás kommutatív lenne (amit most nem is tettünk fel). Csak a „reciprok" szó helyett kell „inverz"-et írnunk. □

2.2.12. Gyakorlat. Mutassuk meg, hogy ha az R egységelemes gyűrű r elemének van balinverze, akkor az r nem baloldali nullosztó.

2.2.15. Állítás. *A $\mathbb{Z}_m$ gyűrű akkor és csak akkor nullosztómentes, ha m prímszám, és ebben az esetben test is.*

Bizonyítás. Ha m összetett szám, azaz $m = ab$, ahol $1 < a, b < m$, akkor $a *_m b = 0$, vagyis nullosztókat találtunk. Ha viszont m prímszám, és $u *_m v = 0$, ahol $0 \leq u, v < m$, akkor $m \mid uv$, és így m prímtulajdonsága miatt $m \mid u$ vagy $m \mid v$. Az első esetben az u, a második esetben a v lesz nulla. Tehát $\mathbb{Z}_m$ nullosztómentes. Az, hogy $\mathbb{Z}_m$ test, ha m prímszám, az alábbi feladat megoldásából következik. □

2.2.13. Feladat. Mutassuk meg, hogy a $\mathbb{Z}_m$ gyűrű egy u eleme akkor és csak akkor invertálható, ha u és m relatív prímek.

Ennek alapján már megérthetjük, hogy a $\mathbb{Z}_5^\times$ csoport, azaz $\mathbb{Z}_5$ multiplikatív csoportja miért az 1, 2, 3, 4 elemekből áll.

A magyar nyelvű szakirodalomban általában *integritási tartománynak* hívják a nullosztómentes és kommutatív gyűrűket. A most következő, polinomokkal kapcsolatos vizsgálatokban elsősorban ilyen gyűrűkkel fogunk foglalkozni, amelyek azonban rendszerint egységelemesek is. Erre nincs bevett magyar terminológia. A rövidség kedvéért szokásos gyűrűnek nevezzük őket.

2.2.16. Definíció. Azt mondjuk, hogy *R szokásos gyűrű*, ha kommutatív, egységelemes és nullosztómentes.

Az utolsó fogalom, amit precízen definiálni szeretnénk, a művelettartás. Erre is sok példát láttunk, ilyen volt a komplex konjugálás, a modulo m maradék képzése, vagy az egységgyököknél használt $k \mapsto \varepsilon_k$ megfeleltetés. Mindezekben az a közös, hogy két halmazon egy-egy művelet van adva, továbbá a két halmaz között egy leképezés. A művelettartás azt fejezi ki, hogy *mindegy az, hogy először a műveletet végezzük el, és azután alkalmazzuk a leképezést, vagy fordítva.*

2.2.17. Definíció. Legyen $\varphi : A \to B$ egy leképezés, továbbá $*$ az A halmazon, $\circ$ pedig a B halmazon értelmezett kétváltozós művelet. Azt mondjuk, hogy φ (ezekre a műveletekre nézve) *művelettartó,* ha tetszőleges $x, y \in A$ esetén

$$\varphi(x * y) = \varphi(x) \circ \varphi(y) .$$

A művelettartás során fontos mindig odafigyelnünk arra, hogy hogy egy adott φ leképezés mely műveleteket tartja. Például legyen R és S két gyűrű. A kettő között haladó $\varphi : R \to S$ leképezést akkor szokás művelettartónak vagy *gyűrűhomomorfizmusnak* nevezni, ha az összeadást és a szorzást is tartja, vagyis ha

$$\varphi(r + s) = \varphi(r) + \varphi(s) \quad \text{és} \quad \varphi(rs) = \varphi(r)\varphi(s) .$$

Szó sincs tehát olyasféle „vegyes" művelettartásról, hogy $\varphi(rs) = \varphi(r) + \varphi(s)$.

A művelettartás (illetve a lényegében ugyanezt kifejező homomorfizmus) az algebra talán legfontosabb fogalma. Ennek az általános fogalomnak azonban most, a polinomok tárgyalásakor még nem lesz akkora jelentősége, mint a gyűrűknek és a testeknek. Ezért az olvasót arra biztatjuk, hogy a művelettartás fenti definícióját vesse össze a korábban szerepelt konkrét példákkal, de ezzel a fogalommal most csak néhány feladat erejéig foglalkozunk.

Gyakorlatok, feladatok

2.2.14. Gyakorlat. Az S halmazon tekintsük az $x * y = x$ képlettel definiált $*$ műveletet. Mutassuk meg, hogy félcsoportot kaptunk, és határozzuk meg a baloldali illetve a jobboldali neutrális elemeket.

2.2.15. Gyakorlat. Az alábbi struktúrák gyűrűk-e? Ha igen, kommutatívak-e, egységelemesek-e, nullosztómentesek-e, testek-e? A kommutatív gyűrűkben határozzuk meg az invertálható elemeket.

(1) $\{a + bi \,:\, a, b \in \mathbb{Q}\}$ a szokásos összeadásra és szorzásra nézve.
(2) $\mathbb{G} = \{a + bi \,:\, a, b \in \mathbb{Z}\}$ a szokásos összeadásra és szorzásra nézve (ezek az úgynevezett *Gauss-egészek*).
(3) $\{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$ a szokásos összeadásra és szorzásra nézve.
(4) $\{a + b\sqrt[3]{2} \,:\, a, b \in \mathbb{Q}\}$ a szokásos összeadásra és szorzásra nézve.
(5) Tetszőleges Abel-csoport, a szorzást úgy definiáljuk, hogy minden szorzat nulla.

(6) Egy X halmaz összes részhalmaza, ahol az összeadás a szimmetrikus differencia képzése, a szorzás pedig a metszetképzés. (Két halmaz szimmetrikus differenciája azokból az elemekből áll, amelyek a két halmaz közül pontosan egyben vannak benne.)

2.2.16. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}_6$ gyűrűben $R = \{0, 2, 4\}$ részgyűrűt alkot. Egységelemes gyűrű-e, illetve test-e az R gyűrű?

2.2.17. Gyakorlat. Bizonyítsuk be tetszőleges a, b valós számokra az alábbi, úgynevezett *binomiális tételt*:

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j} b^j =$$

$$= a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a b^{n-1} + b^n \,.$$

Az állításban szereplő *binomiális együtthatókat* a C.0.12. Tételben definiáltuk. Mutassuk meg, hogy az állítás érvényben marad akkor is, ha az a és b egy tetszőleges R kommutatív gyűrű elemei. Hogyan kell ekkor érteni a binomiális együtthatókkal való szorzást?

2.2.18. Feladat. Jelölje $\mathbb{Z}[\sqrt{2}]$ az $a + b\sqrt{2}$ alakú számok gyűrűjét a $\mathbb{C}$-beli összeadásra és szorzásra, ahol $a, b \in \mathbb{Z}$. Igazoljuk, hogy ebben végtelen sok invertálható elem van.

2.2.19. Feladat. Ha R kommutatív, egységelemes gyűrű, akkor tekintsük az $a + bi$ alakú formális kifejezéseket, ahol $a, b \in R$ (ezeket nevezhetnénk R feletti komplex számoknak). A műveleteket ugyanúgy végezzük, mint a közönséges komplex számok esetén. Testet kapunk-e, ha $R = \mathbb{Z}_3$ illetve ha $R = \mathbb{Z}_5$?

2.2.20. Gyakorlat. Döntsük el az alábbi $\varphi : R_1 \to R_2$ leképezésekről, hogy tartják-e a megadott műveleteket.

(1) $R_1 = \mathbb{R}^+$, $R_2 = \mathbb{R}^\times$, $\varphi(x) = 2^x$.
(2) $R_1 = \mathbb{R}^+$, $R_2 = \mathbb{C}^\times$, $\varphi(x) = \cos x + i \sin x$.
(3) $R_1 = \mathbb{Z}^+_{100}$, $R_2 = \mathbb{Z}^+_{100}$, $\varphi(x) = 60 *_{100} x$.
(4) $R_1 = \mathbb{Z}^+_{100}$, $R_2 = \mathbb{Z}^+_{100}$, $\varphi(x) = 60x$.

2.2.21. Feladat. Legyen $\varphi : G_1 \to G_2$ művelettartó leképezés két csoport között. Mutassuk meg, hogy φ az egységelemet az egységelembe viszi, és inverz képe a kép inverze lesz (azaz φ az inverzképzés műveletét is tartja).

2.2.22. Feladat. Igazoljuk, hogy az $\{a + bi \mid a, b \in \mathbb{Q}\}$ és $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ testek között nincs kölcsönösen egyértelmű, művelettartó (azaz összeg- és szorzattartó) leképezés.

2.2.23. Gyakorlat. Legyen G egy kommutatív csoport, amelyben a műveletet $+$ jelöli, és $a_1, \ldots, a_n \in G$. Igazoljuk, hogy $1 \leq k \leq n$ esetén

$$\sum_{j=1}^{k} a_i + \sum_{j=k+1}^{n} a_i = \sum_{j=1}^{n} a_i \, .$$

Igaznak érezzük ezt akkor is, ha $k = n - 1$? És ha $k = n$? Hány tagja van ebben az esetben a baloldalon szereplő összegeknek? Hogyan érdemes értelmeznünk az egytagú összeget? És a nulla tagú *üres összeget?* Hogyan érdemes definiálni az *üres szorzat*ot?

2.3. A polinomok alaptulajdonságai

Ebben a szakaszban a polinomokra vonatkozó alapvető fogalmakat ismételjük át, de most már olyan általánosságban, ahogy azt a későbbiek megkívánják. Ezután az érdeklődő olvasók számára vázoljuk, hogy hogyan lehet a polinomok fogalmát precízen bevezetni.

2.3.1. Definíció. Legyen R egységelemes, kommutatív gyűrű. Ekkor $R[x]$ jelöli az R-beli együtthatós, x határozatlanú polinomok, vagyis az

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

alakú formális kifejezések halmazát, ahol $a_i \in R$. Ezeket *R fölötti* polinomoknak is mondjuk. Polinomok egyenlőségét, fokát, összegét és szorzatát ugyanúgy definiáljuk, ahogy a 2.1. Szakaszban tettük.

2.3.2. Tétel. *Ha R egységelemes, kommutatív gyűrű, akkor $R[x]$ is az, amely tartalmazza az R gyűrűt, mint konstans polinomokat. Polinomok összegének foka legfeljebb annyi lehet, mint a tagok fokainak maximuma. Ha R nullosztómentes, akkor nem nulla polinomok szorzatának foka a fokok összege lesz. Ilyenkor $R[x]$ is nullosztómentes, és az $R[x]$ (szorzásra) invertálható elemei azok a konstans polinomok, amelyek R-ben invertálhatóak.*

Bizonyítás. A műveleti azonosságokat (asszociativitást, kommutativitást) nem számoljuk ki (kivéve a disztributivitást a 2.3.1. Gyakorlatban). Az $R[x]$ nulleleme nyilván a nullapolinom, egységeleme pedig a konstans 1 polinom, ahol 1 az R egységeleme. Ha R nullosztómentes, akkor a 2.1.3. Állítás bizonyítása most is működik, mert a szorzatpolinom főegyütthatója, mint két nem nulla R-beli elem szorzata, nem lesz nulla. Az összeg és szorzat fokáról szóló állítások is a korábbi módon bizonyíthatók, az invertálható elemek meghatározásához pedig a 2.1.5. Állítás bizonyítása ad mintát. □

E szakasz hátralévő részét (a gyakorlatok kivételével) apró betűs résznek érdemes tekinteni. A komplex számok precíz bevezetését a 1.6. Szakaszban írtuk le. Most ehhez hasonlóan megmutatjuk, hogy hogyan lehet a polinomokat is precízen bevezetni. A két felépítés rendkívül hasonló, de technikailag a komplex számok bevezetése az egyszerűbb, és ezért azt érdemes először elolvasni. Az olvasó a most következőket is nyugodtan átugorhatja a könyv első olvasásakor.

A „formális kifejezés” szemléletes fogalmát nehéz precízen kezelni, és ezért ami most következik, az nem szemléletes, viszont precíz lesz. Amikor majd más struktúrákban (például csoportokban) beszélünk polinomokról, akkor mégsem kerülhetjük meg, hogy a formális kifejezés fogalmát precízzé tegyük. Erre a 8.1. Szakaszban kerül sor.

Abból indulunk ki, ahogy a polinomok egyenlőségét definiáltuk. Egy polinomot az együtthatói határoznak meg, vagyis az $a_0, a_1, a_2, \dots$ számok (vagy általában gyűrűelemek). Mivel a polinom véges sok tagú összeg, az a_j számok valamettől kezdve mindannyian nullák lesznek. Tehát a nem szemléletes, de jól kezelhető definíció a következő:

2.3.3. Definíció. Legyen R kommutatív, egységelemes gyűrű. Ekkor R feletti polinomon egy olyan

$$(a_0, a_1, \dots, a_k, \dots)$$

sorozatot értünk, ahol $a_j \in R$ minden $j \geq 0$ egészre, és van olyan n egész, hogy $j \geq n$ esetén $a_j = 0$. (Természetesen ez az n szám más polinom esetében más lehet.)

Kézenfekvőek ennek alapján a következő fogalmak: nullapolinom (mindegyik $a_j = 0$), polinom foka (ez n, ha $a_n \neq 0$, de a_j már nulla minden $j > n$ esetén), főegyüttható (n-edfokú polinomnál a_n), konstans tag (az a_0). A műveleteket is könnyen definiálhatjuk, hiszen korábban már kiszámoltuk az összeg és szorzat együtthatóit. Ha tehát

$$f = (a_0, a_1, \dots, a_k, \dots) \quad \text{és} \quad g = (b_0, b_1, \dots, b_k, \dots),$$

akkor legyen

$$f + g = (a_0 + b_0, a_1 + b_1, \dots, a_k + b_k, \dots),$$

és

$$fg = (c_0, c_1, \dots, c_k, \dots),$$

ahol c_k értékét a (2.1.1) formula szolgáltatja (43. oldal). Persze le kell ellenőrizni, hogy az összeg és szorzat is polinom-e, azaz, hogy valamettől kezdve csupa nulla elemek szerepelnek-e ebben a két sorozatban, de ez nyilván így van.

A polinomjaink között most nincsenek ott R elemei, hiszen a c elem nem ugyanaz, mint a megfelelő $(c, 0, 0, \dots)$ konstans polinom. Azonban a konstans polinomokkal ugyanúgy kell számolni, mint R elemeivel, hiszen

$$(c, 0, 0, \dots) + (d, 0, 0, \dots) = (c + d, 0, 0, \dots)$$

és

$$(c, 0, 0, \dots)(d, 0, 0, \dots) = (cd, 0, 0, \dots)$$

teljesül az összeadás és a szorzás definíciója miatt. Másképp fogalmazva, a

$$\varphi : c \mapsto (c, 0, 0, \dots)$$

leképezés (amely kölcsönösen egyértelmű R elemei és a konstans polinomok halmaza között) tartja az összeadást és a szorzást is. Ezért a c elemet *azonosítjuk* a neki megfelelő konstans polinommal.

Nincs ott a polinomjaink között az x határozatlan sem. Ha belegondolunk, az x polinom konstans tagja 0, az x-es tag együtthatója 1 (az R egységeleme, ezért volt fontos, hogy R egységelemes legyen), és a többi együttható nulla. Tehát ha a

$$(0, 1, 0, 0, 0, \dots)$$

polinomot x-szel *jelöljük,* akkor a szorzás szabálya miatt

$$x^2 = (0, 0, 1, 0, 0, \dots), \qquad x^3 = (0, 0, 0, 1, 0, 0, \dots),$$

és így tovább, továbbá

$$(c, 0, 0, \dots)x^3 = (0, 0, 0, c, 0, 0, \dots),$$

(és ugyanígy a többi kitevőre is), végül pedig az összeadás definíciója miatt

$$(a_0, a_1, \dots, a_k, \dots) = (a_0, 0, \dots) + (a_1, 0, 0, \dots)x + \dots + (a_k, 0, 0, \dots)x^k + \dots$$

(ez persze csak véges sok tagú összeg, mert valamettől kezdve $a_j = 0$, és innentől kezdve a megfelelő tagokat nem kell kiírni). Mivel $(a_k, 0, 0, \dots)$-t azonosítottuk a_k-val, az

$$a_0 + a_1x + \dots + a_kx^k + \dots$$

alakot kapjuk, ami már a polinomok korábban megszokott formája.

Ezen a ponton tehát visszakapcsolódhatunk a korábbi tárgyalás menetébe, megmutathatjuk, hogy a polinomok tényleg gyűrűt alkotnak, és a többi hasonló állítást is.

Gyakorlatok, feladatok

2.3.1. Gyakorlat. Bizonyítsuk be az $R[x]$ polinomgyűrűben a disztributív azonosságot.

2.3.2. Gyakorlat. Részgyűrűt alkotnak-e

(1) $\mathbb{C}[x]$ páros fokú elemei és a 0 a $\mathbb{C}[x]$-ben?
(2) $\mathbb{R}[x]$ legalább huszadfokú elemei és a 0 az $\mathbb{R}[x]$-ben?

2.3.3. Gyakorlat. Gyűrűt alkotnak-e $\mathbb{C}[x]$ elemei a szokásos összeadásra, és a kompozícióra, mint szorzásra?

2.3.4. Gyakorlat. Legyen m rögzített nemnegatív egész szám. Az $f \in \mathbb{Z}[x]$ polinomhoz rendeljük hozzá azt az $\overline{f} \in \mathbb{Z}_m[x]$ polinomot, amelyet f-ből úgy kapunk, hogy minden együtthatóját modulo m vesszük. Mutassuk meg, hogy az $f \to \overline{f}$ leképezés összeg- és szorzattartó, vagyis gyűrűhomomorfizmus $\mathbb{Z}[x]$-ből $\mathbb{Z}_m[x]$-be.

2.3.5. Gyakorlat. Ha R és S gyűrűk, és $\varphi : R \to S$ gyűrűhomomorfizmus, akkor mutassuk meg, hogy $a_0+a_1x+\dots+a_nx^n \mapsto \varphi(a_0)+\varphi(a_1)x+\dots+\varphi(a_n)x^n$ is gyűrűhomomorfizmus $R[x]$-ből $S[x]$-be.

2.4. Polinomfüggvények és gyökök

Ebben a szakaszban általános polinomokkal foglalkozunk, amelyek együtthatói tetszőlegesek (azaz egy kommutatív, egységelemes R gyűrű elemei) lehetnek. Gyűrűn ezért most kommutatív és egységelemes gyűrűt értünk. Akinek ez az általánosság még nehézséget okoz, az nyugodtan képzelje, hogy az R elemei, vagyis a szereplő polinomok együtthatói (komplex) számok.

A polinomokkal formálisan számolunk ugyan, de sokszor konkrét számokat is be akarunk helyettesíteni az x helyére. Ha $f = a_0 + a_1x + \cdots + a_nx^n$, és $b \in R$, akkor legyen

$$f^*(b) = a_0 + a_1b + \cdots + a_nb^n \in R\,.$$

Ebben a jelölésben a $*$ feleslegesnek látszik (később el is hagyjuk majd). Itt arra szolgál, hogy figyelmeztessen bennünket: a b nem határozatlan immár, hanem egy konkrét R-beli elem. E jelölés azonban azt is mutatja, hogy f^* egy *függvény*nek is felfogható, amely R-ből R-be képez. Ez nem ismeretlen dolog középiskolából sem, hiszen például az x^2 polinomot sokszor függvénynek képzeltük, sőt le is rajzoltuk a grafikonját.

2.4.1. Definíció. Ha $f \in R[x]$ egy polinom, akkor azt az $f^* : R \to R$ függvényt, amelyet a fenti képlet definiál, az f-hez tartozó *polinomfüggvénynek* nevezzük.

Bár egy f polinom, mint formális kifejezés, és az f^* polinomfüggvény nyilván nem ugyanaz, esetleg valaki arra gondolhat, hogy gyakorlati szempontból nincs nagy különbség közöttük, hiszen például az x^2 valós feletti grafikonjából visszakaphatjuk az x^2 polinomot. Nézzük meg, igaz marad-e ez, ha a $\mathbb{Z}_2$ gyűrű felett dolgozunk. Ennek csak két eleme van, így a „grafikon” mindössze két pontból áll. A polinomfüggvényeket tehát táblázatosan is megadhatjuk:

f	$f^*(0)$	$f^*(1)$
x^2	0	1
x^3	0	1
x	0	1
$x+1$	1	0
0	0	0
x^2+x	0	0
1	1	1
x^2+x+1	1	1

Itt bizony sok egybeesés van, például az x, x^2 és x^3 polinomokhoz is ugyanaz a polinomfüggvény tartozik. Persze ez nem meglepő: a $\{0, 1\}$ halmazból önmagába csak négy függvény létezik egyáltalán, hiszen 0-nál is és 1-nél is csak kétféle függvényérték lehetséges. Mind a négy lehetséges függvény szerepel is a fenti táblázatban, azaz $\mathbb{Z}_2$ *fölött minden függvény polinomfüggvény.* Polinom viszont végtelen sok van $\mathbb{Z}_2$ fölött (például

$x, x^2, x^3, \ldots, x^k, \ldots$ csupa különböző polinomok). Egyik fontos célunk, hogy megvizsgáljuk: milyen összefüggés van általában egy polinom és a hozzá tartozó polinomfüggvény között, mikor határozza meg az utóbbi az előbbit.

Első lépésként vizsgáljuk meg, hogy mit kapunk eredményül, ha összeg- illetve szorzatpolinomba helyettesítünk. A polinomok közötti műveleteket pontosan azzal a szándékkal definiáltuk, hogy az alábbi állítás igaz legyen.

2.4.1. Gyakorlat. Mutassuk meg, hogy ha $f, g \in R[x]$, és $b \in R$, akkor

$$(f+g)^*(b) = f^*(b) + g^*(b) \qquad \text{és} \qquad (fg)^*(b) = f^*(b)g^*(b)\,.$$

A középiskolában függvényekkel is végeztünk műveleteket. Például az $x \sin x$ az a függvény volt, ami az x helyen az x és a $\sin x$ szorzatát veszi fel. Ennek alapján a polinomfüggvények összegét és szorzatát is definiálhatjuk. Az alábbi definíció megemésztéséhez nagyon ajánljuk a 2.4.15. Gyakorlatot.

2.4.2. Definíció. Legyen R gyűrű, és p, q két függvény, ami R-et R-be képzi. Ekkor $p+q$ illetve pq az a függvény, ami tetszőleges $b \in R$ helyen $p(b) + q(b)$-t, illetve $p(b)q(b)$-t vesz fel. Képletben:

$$(p+q)(b) = p(b) + q(b) \qquad \text{és} \qquad (pq)(b) = p(b)q(b)\,.$$

Az $f+g$ illetve fg neve az f és g függvények *pontonkénti* összege illetve szorzata.

Most egy viszonylag gyors eljárást mutatunk polinomba való behelyettesítésre. Példaként legyen $f(x) = 3x^4+2x^3+x+2$, és helyettesítsünk be $b = 2$-t. A szükséges szorzások számát nagymértékben lecsökkenthetjük, ha a polinomot a következőképpen alakítjuk át:

$$f(x) = \Big(\big((3x+2)x+0\big)x+1\Big)x+2$$

A részletszámításokat „belülről kifelé haladva” egy táblázatba írjuk:

	3	2	0	1	2
$b=2$	3	$2\cdot 3+2=8$	$2\cdot 8+0=16$	$2\cdot 16+1=33$	$2\cdot 33+2=68=f^*(b)$

Az eljárás tehát a következő:

(1) A táblázat felső sorába felírjuk sorban a polinom együtthatóit, a főtagtól a konstans tagig. (Vigyázzunk közben arra, hogy a nulla együtthatókat is be kell írni a táblázatba, akkor is, ha azokat a polinomban nem írtuk ki.)
(2) Az alsó sorba bemásoljuk a főegyütthatót, a főegyüttható alá. A sor elejére oda szokás írni a behelyettesítendő b értéket is.
(3) Az alsó sort balról jobbra haladva töltjük ki. Az utoljára kitöltött mezőben talált értéket megszorozzuk b-vel, majd hozzáadjuk a következő, üres mező fölött található együtthatót, és az eredményt beírjuk ebbe az üres mezőbe.
(4) Az $f^*(b)$ értékét az alsó sor végéről olvashatjuk le.

Általában tehát a következő, úgynevezett *Horner-elrendezést* kapjuk:

	a_n	$\dots$	a_{j+1}	a_j	$\dots$	a_1	a_0
b	$c_{n-1} = a_n$	$\dots$	c_j	$c_{j-1} = bc_j + a_j$	$\dots$	c_0	$f^*(b) = bc_0 + a_0$

2.4.2. Gyakorlat. Mutassuk meg általában is, hogy a Horner-elrendezés az $f^*(b)$ értéket számítja ki. Igazoljuk az alábbi összefüggést:

$$f(x) = (x-b)(c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0) + f^*(b)\,,$$

ahol $f(x) = a_nx^n + \cdots + a_0$, és $c_{n-1}, \dots, c_0$ a táblázatban kiszámított értékek.

Ezek szerint minden $f \in R[x]$ polinom tetszőleges $b \in R$ esetén felírható

$$f(x) = (x-b)q(x) + f^*(b)$$

alakban alkalmas $q \in R[x]$ polinomra. Ezt az észrevételt (amely önmagában is elegendő a következő állítás bizonyításához) később általánosítani fogjuk, amikor a polinomok közötti *maradékos osztásról* beszélünk majd a 3.2. Szakaszban.

2.4.3. Definíció. Azt mondjuk, hogy $b \in R$ *gyöke* az $f \in R[x]$ polinomnak, ha $f^*(b) = 0$.

2.4.4. Állítás. *A $b \in R$ akkor és csak akkor gyöke az $f \in R[x]$ polinomnak, ha*

$$f(x) = (x-b)q(x)$$

alkalmas $q \in R[x]$ polinomra.

Bizonyítás. Ha f ilyen alakban írható, akkor b nyilvánvalóan gyöke f-nek. Megfordítva, ha b gyöke f-nek, akkor a Horner-elrendezés alsó sorában szereplő számok egy megfelelő q polinom együtthatóit szolgáltatják (a 2.4.2. Gyakorlat miatt). □

Ha b gyöke f-nek, akkor az $x - b$ kifejezést az f polinom b-hez tartozó *gyöktényezőjének* nevezzük, az előző állítás a *gyöktényező kiemelhetőségéről szóló tétel*.

Ha egy polinomnak több gyöke is van, akkor megpróbálhatunk egyszerre több gyöktényezőt is kiemelni. Ehhez nagyon fontos, hogy az R gyűrű *nullosztómentes* legyen. Ha ez nem teljesül, akkor furcsa dolgok történhetnek. Például a $\mathbb{Z}_8$ gyűrű felett tekintsük az $x^2 - 1$ polinomot. Ennek gyökeit akár úgy is megállapíthatjuk, hogy végigpróbálgatjuk a $\mathbb{Z}_m$ nyolc elemét. Az eredmény, hogy ennek gyökei a négy páratlan szám, azaz 1, 3, 5, 7. A gyöktényezőket kiemelve azonban *kétféle* felbontást kapunk:

$$x^2 - 1 = (x-1)(x-7) = (x-3)(x-5)\,.$$

A polinom tehát két, lényegesen különböző módon is felbontható gyöktényezők szorzatára, és egyszerre csak két gyöktényezőt tudunk szerepeltetni a lehetséges négy közül. A problémát az okozza, hogy ha az $(x-1)(x-7)$ alakba az $r = 3$ gyököt behelyettesítjük, akkor $0 = 2 *_8 4$ adódik, tehát a nullosztómentesség hiánya teszi lehetővé, hogy az 1-en és a 7-en kívül még legyen gyök.

2.4.5. Tétel. *Egy nullosztómentes R gyűrű (speciálisan egy test) felett a gyöktényezők egyszerre is kiemelhetők: minden nem nulla $f \in R[x]$ polinom felírható*

$$f(x) = (x - b_1) \dots (x - b_k)q(x)$$

alakban, ahol a (nem feltétlenül különböző) $b_1, \dots b_k$ az f-nek az ***összes*** *R-beli gyökei, és q-nak egyáltalán nincs gyöke R-ben. Ezért* ***nullosztómentes gyűrű felett egy polinomnak legfeljebb annyi gyöke lehet, mint a foka.***

Bizonyítás. Egy gyöktényező kiemelésekor a fok eggyel csökken (hiszen nullosztómentes gyűrűben polinomok szorzásakor a fokok összeadódnak). Emeljünk ki f-ből addig gyöktényezőket, ameddig lehet. Vagyis ha

$$f(x) = (x - b_1) \dots (x - b_m)q_m(x)\,,$$

de q_m-nek még van gyöke R-ben, akkor q_m-ből emeljünk ki egy további gyöktényezőt. Ezt csak véges sokszor lehet csinálni, mert q_m foka minden lépésnél csökken. Ezért előbb-utóbb eljutunk az

$$f(x) = (x - b_1) \dots (x - b_k)q(x)$$

alakhoz, ahol már q-nak nincs gyöke R-ben. Ha b gyöke f-nek, akkor ezt behelyettesítve

$$0 = (b - b_1) \dots (b - b_k)q^*(b)$$

adódik. Mivel R nullosztómentes, valamelyik tényező nulla. De $q^*(b) \neq 0$, tehát van olyan j, hogy $b - b_j = 0$, azaz $b = b_j$. Megfordítva, a b_j nyilván gyöke f-nek (hiszen az R gyűrűben a nullát bármelyik elemmel szorozzuk meg, nullát kapunk). Tehát f gyökei pontosan $b_1, \dots, b_k$.

Az utolsó állítás bizonyításához írjuk fel a fokszámokat:

$$\mathrm{gr}(f) = \mathrm{gr}(x - b_1) + \dots + \mathrm{gr}(x - b_k) + \mathrm{gr}(q) = k + \mathrm{gr}(q).$$

Ezért tényleg $\mathrm{gr}(f) \geq k$. □

2.4.3. Gyakorlat. Az előző bizonyításban mely állítások maradnak érvényesek, ha az R gyűrűről nem tesszük fel a nullosztómentességet? A fokszámokkal kapcsolatos érvelésekénél is kihasználtuk-e a nullosztómentességet, vagy csak b behelyettesítésekor?

Most már könnyű belátni, hogy ha két polinom „elég sok” helyen megegyezik, akkor azonosak.

2.4.6. Következmény [A polinomok azonossági tétele]. *Ha egy R nullosztómentes gyűrű felett adott két, legfeljebb n-edfokú polinom, amelyek több mint n (R-beli) helyen megegyeznek, akkor a két polinom egyenlő (vagyis együtthatóik is megegyeznek).*

Bizonyítás. Legyen f és g a két polinom. Ha $f - g$ nem a nullapolinom, akkor van foka, ami legfeljebb n lehet. Ugyanakkor $f - g$-nek gyöke minden olyan $b \in R$, ahol f és g megegyezik (azaz $f(b) = g(b)$). Tehát $f - g$-nek több, mint n gyöke van, de foka legfeljebb n, és ez ellentmond az előző tételnek. Az ellentmondást abból kaptuk, hogy feltettük: $f - g$ nem a nullapolinom. Ezért $f - g$ a nullapolinom, azaz $f = g$. □

Ez a bizonyítás akkor is működik, ha f vagy g a nullapolinom, noha a tételben ezt elvileg nem engedtük meg, mert f és g fokáról beszéltünk. Néha ezért megállapodnak abban, hogy (noha a nullapolinomnak nincs foka), a legfeljebb n-edfokú polinomok közé mégiscsak odaértjük a nullapolinomot is. Egy ilyesfajta megállapodás sokat egyszerűsíthet egy-egy tétel szövegén, és könnyebben megjegyezhetővé teheti azt.

2.4.7. Következmény. *Végtelen nullosztómentes gyűrű felett minden polinomot egyértelműen meghatároz a hozzá tartozó polinomfüggvény, véges gyűrű felett viszont nem.*

Bizonyítás. Ha R végtelen, és $f^* = g^*$, akkor f és g végtelen sok helyen megegyezik (mert R minden elemén megegyezik). Tehát az azonossági tétel miatt $f = g$. Ha R véges, akkor csak véges sok függvény van R-ből R-be, tehát csak véges sok polinomfüggvény van. Polinom viszont végtelen sok van, tehát nem tartozhat minden polinomhoz más és más polinomfüggvény. □

A polinomfüggvények tárgyalását ezzel befejeztük. Reménykedvén, hogy már mindenki pontosan érti a különbséget polinom és polinomfüggvény között, ezentúl jelölésben nem különböztetjük meg a kettőt, például egyszerűen $f(r)$-rel jelöljük az f polinom r helyen felvett helyettesítési értékét. Zárásként röviden, két feladat formájában, megemlítjük az *interpoláció* problémáját.

Olyan polinomfüggvényt fogunk keresni, amely adott helyeken adott értékeket vesz fel. Ezek a helyek egy T test páronként különböző elemei, jelölje őket $a_1, \ldots, a_n$, a felveendő értékeket pedig $b_1, \ldots, b_n$. Az azonossági tétel miatt a legfeljebb $n-1$-edfokú polinomok között legfeljebb egy olyan f polinom létezik, melyre $f(a_j) = b_j$ minden j-re. Meg fogjuk mutatni, hogy mindig van ilyen polinom. A legegyszerűbb konstrukció a *Lagrange-interpoláció,* amit a következő feladatban írunk le.

2.4.4. Gyakorlat. Legyenek $a_1, \ldots, a_n$ páronként különböző elemei a T testnek.

(1) Melyek azok az $n-1$-edfokú polinomok, melyeknek az a_j kivételével az $a_1, \ldots, a_n$ mindegyike gyöke?
(2) Melyik az az f_j polinom, ami az előző (1)-beli kívánalmakon kívül még azt is teljesíti, hogy $f_j(a_j) = 1$?
(3) Ha $b_1, \ldots, b_n \in T$, akkor hogyan lehetne az f_j polinomokból és a b_j elemekből egy olyan f polinomot összekombinálni, amelyre $f(a_j) = b_j$ minden j-re?

E módszer előnye, hogy a keresett interpolációs polinomra képletet kapunk. Hátránya viszont a következő. Képzeljük el, hogy az interpoláció célja az, hogy mérési eredményekhez polinomot illesszünk. Ha új mérési eredmény érkezik, akkor a Lagrange-féle technikával elölről kell kezdenünk a számolást. *Newton módszere* azt teszi lehetővé, hogy a már meglevő polinomunkat módosítsuk, hogy az új helyen is a kívánt értéket vegye fel.

2.4.5. Gyakorlat. Tegyük fel, hogy a legfeljebb $n-2$-edfokú f polinom teljesíti, hogy $f(a_j) = b_j$, ha $j = 1, 2, \ldots, n-1$.

(1) Mi az általános alakja az olyan $n-1$-edfokú g polinomoknak, melyekre teljesül, hogy $f+g$ az a_j helyen szintén a b_j értéket veszi fel, ha $j=1,2,\ldots,n-1$?
(2) Hogyan kell g-t megválasztani, hogy $(f+g)(a_n)=b_n$ is teljesüljön?

Többváltozós függvényeket többhatározatlanú polinomokkal interpolálhatunk, erről a 2.6.5. Feladatban lesz szó.

Gyakorlatok, feladatok

2.4.6. Gyakorlat. A Horner elrendezés segítségével döntsük el, hogy a 2 szám gyöke-e az $f(x)=x^6-4x^4+x^3-x^2+4$ polinomnak, és írjuk is fel $f(x)$-et $(x-2)g(x)+f(2)$ alakban.

2.4.7. Gyakorlat. Az $a^k-b^k=(a-b)(a^{k-1}+a^{k-2}b+\cdots+b^{k-1})$ ismert (és beszorzással igazolható) azonosság felhasználásával adjunk új bizonyítást a gyöktényező kiemelhetőségéről szóló tételre (2.4.4. Állítás).

2.4.8. Feladat. Mely m-ekre van $\mathbb{Z}_m[x]$-ben olyan polinom, amelynek több gyöke van, mint a foka?

2.4.9. Feladat. Adjunk meg minden véges test felett olyan polinomot, amelynek nincs gyöke az adott testben.

2.4.10. Gyakorlat. Adjunk meg olyan komplex együtthatós polinomot, amelyre $f(0)=3$, $f(1)=3$, $f(4)=15$ és $f(-1)=0$.

2.4.11. Feladat. Tegyük fel, hogy az $f\in\mathbb{C}[x]$ polinom minden racionális helyen racionális értéket vesz fel. Következik-e ebből, hogy f racionális együtthatós? Igaz-e az állítás, ha „racionális” helyett mindenütt „egész” szerepel?

2.4.12. Feladat. Létezik-e olyan $f\in\mathbb{Z}[x]$ polinom, melyre $f(10)=400$, $f(14)=440$ és $f(18)=520$?

2.4.13. Feladat. Tegyük fel, hogy n egész alapponthoz keresünk interpolációs polinomot, és az itt felvett értékek maguk is egészek, de a kapott legfeljebb $n-1$-edfokú interpolációs polinom mégsem egész együtthatós. Lehetséges-e, hogy az interpoláció egy magasabb fokú, de egész együtthatós polinommal is elvégezhető?

2.4.14. Feladat. Mutassuk meg, hogy ha R kommutatív, egységelemes gyűrű, amely felett az interpoláció korlátlanul elvégezhető, akkor R test.

2.4.15. Gyakorlat. Legyen R (mint eddig is) kommutatív, egységelemes gyűrű. Ellenőrizzük az alábbi állításokat.

(1) Az R-ből R-be menő függvények egységelemes, kommutatív gyűrűt alkotnak a pontonkénti összeadásra és szorzásra (2.4.2. Definíció), ami nem nullosztómentes.
(2) Ez az összeadás és szorzás nem vezet ki a polinomfüggvények közül, és azok is egységelemes, kommutatív gyűrűt alkotnak erre a két műveletre.

(3) Ha $b \in R$ egy rögzített elem, akkor az $f \mapsto f^*(b)$ leképezés összeg- és szorzattartó az $R[x]$ és az R gyűrűk között (röviden: a b behelyettesítése gyűrűhomomorfizmus).
(4) Igazoljuk, hogy az $f \mapsto f^*$ leképezés összeg- és szorzattartó az $R[x]$ és a polinomfüggvények gyűrűje között (azaz a polinomfüggvény képzése gyűrűhomomorfizmus).

2.4.16. Feladat. Legyen R a valós számokon értelmezett, valós értékű függvények gyűrűje a pontonkénti műveletekre. Mutassuk meg, hogy R-nek van olyan S részgyűrűje, amely egységelemes, de S egységeleme nem ugyanaz, mint R egységeleme. Előfordulhat ez a jelenség nullosztómentes R gyűrűben is? (Lásd a 2.2.16. Gyakorlatot is.)

2.5. A gyöktényezős alak

Az előző szakaszban láttuk, hogy ha R nullosztómentes (és mint polinomok vizsgálatakor lényegében mindig, kommutatív és egységelemes) gyűrű, akkor egy polinom gyökeihez tartozó gyöktényezők egyszerre is kiemelhetők. A 2.4.5. Tételben akár olyan szerencsénk is lehet, hogy q már konstans polinom, azaz a végeredmény a következő lesz:

$$f(x) = c(x - b_1)(x - b_2)\dots(x - b_n)\,,$$

ahol c egy nem nulla konstans. Ezt az f *gyöktényezős alakjának* hívjuk.

2.5.1. Gyakorlat. Mutassuk meg, hogy a gyöktényezős alakban szereplő c az f polinom főegyütthatója, az n szám pedig az f foka.

Ez a „szerencse” szükségszerűen bekövetkezik, ha az R gyűrűben minden nem konstans polinomnak már van gyöke.

2.5.2. Feladat. Mutassuk meg, hogy ha egy R (egységelemes, kommutatív) gyűrűben minden nem konstans polinomnak van gyöke, akkor R test.

2.5.1. Definíció. Azt mondjuk, hogy a T test *algebrailag zárt,* ha $T[x]$ minden nem konstans polinomjának van T-ben gyöke.

Algebrailag zárt test fölött tehát minden polinom gyöktényezős alakban írható. A valós számok teste nem algebrailag zárt, hiszen például az $x^2 + 1$ polinomnak nincsen benne gyöke. Pontosan azért vezettük be a komplex számokat, hogy ezt a problémát kiküszöböljük. Láttuk, hogy a komplex számok testében a gyökvonás mindig elvégezhető, vagyis az $x^n - a$ polinomnak mindig van gyöke. A komplex számok konstrukciója azonban még ennél is jobban sikerült.

2.5.2. Tétel [Az algebra alaptétele]. *A komplex számok teste algebrailag zárt.*

Ezt a tételt csak később, a Galois-elmélet egy alkalmazásaként bizonyítjuk. Rá kell azonban mutatnunk, hogy az algebra alaptétele valójában az analízis tétele! Ennek az az oka, hogy a valós számok bevezetésekor folytonossági meggondolások játszanak szerepet. A komplex számokon értelmezett függvények vizsgálatában is fontos szerepet kap az analízis. A komplex függvénytan apparátusával az algebra alaptételére több, nagyon egyszerű, és roppant elegáns bizonyítást kaphatunk.

A gyöktényezős alakban ugyanaz a tényező többször is szerepelhet. Ha ezeket összevonjuk, akkor a következő alakot kapjuk:

$$f(x) = c(x - d_1)^{k_1}(x - d_2)^{k_2} \dots (x - d_m)^{k_m} ,$$

ahol a $d_1, \dots, d_m$ már páronként különbözők. Ezt az összevont formát *kanonikus alaknak* nevezzük, a k_j számot pedig a d_j gyök *multiplicitásának* hívjuk. Másképp fogalmazva azt mondjuk, hogy d_j az f-nek k_j*-szeres gyöke*. A fokszámokat felírva látjuk, hogy

$$k_1 + k_2 + \dots + k_n = \mathrm{gr}(f) .$$

Ezt úgy szokás fogalmazni, hogy egy polinomnak, ha gyöktényezős alakra hozható, *multiplicitásokkal számolva pontosan annyi gyöke van, mint a foka.*

Ezekkel az elnevezésekkel súlyos probléma lenne, ha az f polinomot máshogy is fel tudnánk írni gyöktényezős alakban. Ha előfordulhatna olyasmi, hogy $(x-1)^2(x-2)^3 = (x-1)^3(x-2)^2$ akkor nem tudhatnánk, hogy a 2 szám most kétszeres, vagy háromszoros gyök-e. Ilyesmi azonban nem fordulhat elő, mert *a kanonikus alak egyértelmű,* amit azonnal be fogunk látni.

A többszörös gyökök fenti definíciójával más baj is van: nem elég általános. Ha valós együtthatós polinomokat akarunk vizsgálni, akkor az

$$f(x) = (x-1)^2(x-2)^3(x^2+1)^2(x^2+3)^5$$

ugyan nem hozható kanonikus alakra $\mathbb{R}$ fölött, mégis úgy érezzük, hasznos lenne azt mondani, hogy e polinomnak a 2 szám háromszoros gyöke. Mi lenne akkor a többszörös gyök „helyes" definíciója? Azt érdemes észrevenni, hogy ha a fenti polinomból elvesszük az $(x-2)^3$ gyöktényezőt, akkor a maradék résznek a 2 már nem gyöke.

2.5.3. Definíció. Legyen R szokásos gyűrű. Azt mondjuk, hogy az $f \in R[x]$ polinomnak a $b \in R$ elem k*-szoros gyöke* (vagy, hogy a b gyök *multiplicitása* k), ha

$$f(x) = (x - b)^k q(x)$$

alakban írható, ahol a $q \in R[x]$ polinomnak b már nem gyöke.

Itt k nemnegatív egészet jelöl. Célszerű megengedni a $k = 0$ esetet is, mert így könnyebben fogalmazhatunk meg majd bizonyos eredményeket. Persze a „nullaszoros gyök" helyett azt mondjuk majd, hogy b „nem gyöke" a polinomnak.

2.5.3. Gyakorlat. Mutassuk meg, hogy ha R nullosztómentes, akkor

(1) gyök multiplicitása egyértelműen meghatározott (vagyis az előző definíció adott f és b mellett csak egyetlen k-ra teljesülhet);

(2) ha az f polinomnak van gyöktényezős alakja, akkor a többszörös gyök most adott definíciója ugyanaz, mint amiről fentebb beszéltünk.

Ebből már nyilvánvaló, hogy egy nullosztómentes gyűrű felett a kanonikus alak egyértelmű (ezt más eszközökkel újra belátjuk majd, amikor a polinomok számelméletét tanulmányozzuk). Valóban, a fenti kanonikus alakban a d_j elemek azért egyértelműen meghatározottak, mert ezek pontosan f gyökei, a k_j kitevők pedig az előbbi 2.5.3. Gyakorlat miatt lesznek egyértelműek. Többszörös gyökök meghatározására két eljárást is tanulunk majd (a 3.6, illetve 3.7. Szakaszokban).

Utolsó témaként a *gyökök és együtthatók közötti összefüggéseket* tekintjük át.

2.5.4. Gyakorlat. Számítsuk ki x alábbi két polinomjának az együtthatóit:

$$(x-b_1)(x-b_2)(x-b_3) \qquad \text{és} \qquad (x-b_1)(x-b_2)(x-b_3)(x-b_4)\,.$$

Az előző gyakorlat megoldását általában végezve a következő képleteket kapjuk.

2.5.4. Tétel. *Ha az R kommutatív, egységelemes gyűrű feletti f polinomra*

$$f(x) = (x-b_1)\dots(x-b_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - + \dots + (-1)^n \sigma_n\,,$$

akkor a gyökök és együtthatók közötti összefüggések a következők:

$$\sigma_1 = b_1 + b_2 + \dots + b_n \qquad \text{tagok száma: } \binom{n}{1} = n$$

$$\sigma_2 = b_1b_2 + \dots + b_1b_n + b_2b_3 + \dots + b_{n-1}b_n \qquad \text{tagok száma: } \binom{n}{2}$$

$$\sigma_k = b_1b_2\dots b_k + \dots \qquad \text{tagok száma: } \binom{n}{k}$$

$$\sigma_n = b_1b_2\dots b_n \qquad \text{tagok száma: } \binom{n}{n} = 1\,.$$

A σ_k úgy keletkezik, hogy a $b_1, \dots, b_n$ közül az összes lehetséges módon kiválasztunk k darabot, a kiválasztott b_i-ket összeszorozzuk, majd a kapott szorzatokat összeadjuk. Szokás a σ_0-ról is beszélni, és (a fenti f főegyütthatójaként) konstans 1-nek tekinteni.

(Az itt szereplő $\binom{n}{k}$ binomiális együtthatót a C.0.12. Tételben definiáltuk.) A most kapott képletekben hasznos lesz, ha $b_1, \dots, b_n$-et határozatlanoknak, és nem R-beli elemeknek tekintjük. Ekkor σ_k ezen határozatlanok (többhatározatlanú) polinomjává válik. Ezeket később *elemi szimmetrikus polinomoknak* fogjuk nevezni.

Célszerű a gyökök és együtthatók összefüggését általános együtthatójú polinomra is átfogalmazni.

2.5.5. Következmény. *Tegyük fel, hogy*

$$f(x) = a_0 + a_1x + \dots + a_nx^n = a_n(x-b_1)\dots(x-b_n)\,.$$

Ekkor $0 \le k \le n$ *esetén*

$$a_k = a_n(-1)^{n-k}\sigma_{n-k}(b_1, \dots, b_n)\,,$$

vagyis

$$\sigma_k(b_1, \dots, b_n) = (-1)^k a_{n-k}/a_n\,.$$

Bizonyítás. Az állítás azonnal adódik, ha az $(x - b_1)\dots(x - b_n)$ szorzatot az előző tétel szerint kifejtjük, és a két oldal együtthatóit összehasonlítjuk. □

Gyakorlatok, feladatok

2.5.5. Gyakorlat. Írjuk fel az $x^4 + 4$ polinomot gyöktényezős alakban, és ellenőrizzük beszorzással az eredményt. Hogyan lehetne ezt a polinomot valós együtthatós polinomok szorzatára bontani?

2.5.6. Gyakorlat. Hányszoros gyöke az $x^4 - x^3 - x + 1$ polinomnak az 1? A Horner-elrendezést használjuk.

2.5.7. Gyakorlat. Igazoljuk, hogy ha két n-edfokú komplex együtthatós polinom n (komplex) helyen megegyezik, és a főegyütthatóik egyenlők, akkor a polinomok is egyenlők.

2.5.8. Feladat. Fejezzük ki az $x_1^2 + x_2^2 + \dots + x_n^2$ négyzetösszeget a $\sigma_1(x_1, x_2, \dots, x_n)$ és a $\sigma_2(x_1, x_2, \dots, x_n)$ segítségével.

2.5.9. Gyakorlat. Határozzuk meg a $2x^4 + 2x + 3$ polinom komplex gyökeinek összegét, szorzatát, négyzetösszegét, és a gyökök reciprokainak összegét.

2.5.10. Feladat. Legyenek $\varepsilon_1, \dots, \varepsilon_n$ az összes n-edik egységgyökök.

(1) Bontsuk gyöktényezős alakra az $x^4 - 1$ polinomot.
(2) Bizonyítsuk be, hogy $x^n - 1 = (x - \varepsilon_1)\dots(x - \varepsilon_n)$.
(3) A gyökök és együtthatók összefüggése alapján számítsuk ki az n-edik egységgyökök összegét, négyzetösszegét és szorzatát.
(4) Az egységsugarú körbe írt szabályos n-szög egy csúcsából az összes többi csúcsba húzott szakaszok hosszát összeszoroztuk. Bizonyítsuk be, hogy az eredmény n-nel egyenlő.

2.5.11. Gyakorlat. Értelmezhető-e egy polinomfüggvény gyökeinek a multiplicitása?

2.6. Többhatározatlanú polinomok

Ahogy korábban már megbeszéltük, többhatározatlanú polinomon olyan kifejezéseket szeretnénk érteni, amelyek az $x_1, \ldots, x_n$ határozatlanokból és valamilyen R gyűrű elemeiből épülnek fel összeadás, kivonás és szorzás segítségével. Azt gondoljuk, hogy ezek

$$f(x_1, \ldots, x_n) = \sum r_{m_1,m_2,\ldots,m_n} x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$$

alakban írhatók fel, ahol az $r_{m_1,m_2,\ldots,m_n}$ együtthatók R-nek elemei, $m_1, m_2, \ldots, m_n$ pedig nemnegatív egészek. A polinom *tagjainak* a fenti összeg tagjait nevezzük (feltételezve, hogy a lehetséges összevonásokat már elvégeztük, tehát semelyik $x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ sem szerepelhet több együtthatóval). Azt szeretnénk, hogy ezeket az együtthatókat a polinom egyértelműen meghatározza. Láttuk (a 2.1. Szakasz végén) azt is, hogy magát a definíciót érdemesebb úgy megalkotni, hogy a fenti „polinomot" az egyik határozatlan szerint rendezzük. Ekkor az együtthatók is polinomok lesznek, amelyekben azonban már eggyel kevesebb a határozatlan.

2.6.1. Definíció. Az R (kommutatív, egységelemes) gyűrű feletti, $x_1, \ldots x_n$-határozatlanú (vagy röviden csak n-határozatlanú) polinomok $R[x_1, \ldots, x_n]$ gyűrűjét n szerinti indukcióval definiáljuk: ez nem más, mint $(R[x_1, \ldots, x_{n-1}])[x_n]$. Az indukció kezdőlépése a már ismert $R[x_1]$ polinomgyűrű.

Ebben a definícióban úgy képzeltük, hogy a polinomokat az x_n határozatlan szerint rendezzük. Eszünkbe juthatna, hogy mondjuk az x_1 határozatlan szerint rendezzük őket, és akkor az $R[x_2, \ldots, x_n][x_1]$ gyűrűhöz jutnánk. Ez formailag más, mint az $R[x_1, \ldots, x_{n-1}][x_n]$ (pláne ha még a „sorozatos" precíz bevezetéshez is ragaszkodunk). De a két gyűrű mégis, a lényeget tekintve ugyanaz. (Később az ilyesmit úgy fogalmazzuk majd, hogy a két gyűrű *izomorf,* lényegében „ugyanazok" az elemeik, és „ugyanúgy" kell bennük számolni, precízen: van közöttük kölcsönösen egyértelmű, művelettartó megfeleltetés.) Most azonban minderre még semmi szükség nincs, mert a fenti többértelműség semmiféle gyakorlati problémát nem fog okozni.

2.6.2. Állítás. *Az n-határozatlanú polinomok gyűrűje kommutatív és egységelemes. Ha R nullosztómentes, akkor $R[x_1, \ldots, x_n]$ is az, és az invertálható elemei azok a konstans polinomok, amelyek R-ben invertálhatóak.*

Bizonyítás. Teljes indukcióval azonnal következik a 2.3.2. Tételből. Természetesen a konstans polinomok továbbra is R elemei, amelyeket (sőt az n-nél kevesebb határozatlanú polinomokat is) n-határozatlanú polinomoknak képzeljük. □

A fenti $r x_1^{m_1} x_2^{m_2} \ldots x_n^{m_m}$ tag *fokát* $m_1 + \cdots + m_m$-nek definiáljuk. Az f polinom fokán a benne szereplő tagok fokainak maximumát értjük. Vigyázzunk, ez *nem ugyanaz*, mint amikor a polinomot mondjuk x_n polinomjának tekintve számítjuk ki a fokát. Például

$$f = x^2 y + y^3 x$$

foka 2, ha f-et x polinomjának tekintjük, 3, ha y polinomjának tekintjük, és 4 a fenti értelemben. Tehát ha fokszámról beszélünk, mindig meg kell mondanunk, milyen értelemben gondoljuk, vagyis hogy a polinomot többhatározatlanúnak, vagy egyhatározatlanúnak képzeljük (és az utóbbi esetben melyik határozatlan szerint rendezünk).

Egy polinomot *homogénnek* nevezünk, ha minden tagjának ugyanaz a foka. Ha f polinom, akkor gyűjtsük össze a k-adfokú tagjait, és jelöljük ezek összegét f_k-val. Nyilván f_k homogén polinom, és f az f_k polinomok összege. Ezért minden polinom egyértelműen felbontható homogén polinomok összegére. Az f_k-t az f polinom k-adfokú *homogén komponensének* hívjuk.

Ha f-ben nincs egyáltalán k-edfokú tag, akkor f_k-t nullának értjük (lásd az üres összegről írottakat a 2.2.23. Gyakorlatban).

2.6.1. Gyakorlat. Mutassuk meg, hogy ha f és g többhatározatlanú polinomok az R nullosztómentes gyűrű fölött, akkor az fg polinom k-adfokú homogén komponense

$$f_0 g_k + f_1 g_{k-1} + \cdots + f_k g_0 = \sum_{i=0}^{k} f_i g_{k-i} \,.$$

Speciálisan fg foka az f és g fokainak összege.

A következő szakaszban belátjuk első komolyabb tételünket, az úgynevezett szimmetrikus polinomok alaptételét. A bizonyításhoz egy új fogalom bevezetésére van szükség: általánosítanunk kell a főtag fogalmát többváltozós polinomokra.

Vegyünk egy $f \in R[x_1, \ldots, x_n]$ polinomot, ennek tagjai $r x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ alakúak. A kitevők $(m_1, \ldots, m_n)$ sorozatát egy n „jegyű” telefonszámnak képzelhetjük (az analógia annyiban sántít, hogy a „jegyek”, vagyis az m_j számok akármekkorák lehetnek). Rakjuk ezeket a telefonszámokat növekvő sorrendbe a szokásos módon, és írjuk fel az f polinom tagjait ebben a sorrendben. Például ha

$$f(x_1, x_2, x_3) = x_1 x_2^4 - i x_1^2 x_3 + x_1 x_2 x_3 - 3x_2^3 + x_3^2 + 2x_1^2 + x_1 x_2 x_3^3 \,,$$

akkor a kapott „telefonszámok” $x_1 x_2^4 = x_1 x_2^4 x_3^0 \mapsto 140$ (a nulla kitevőket is ki kell írni!), azután sorban haladva 201, 111, 030, 002, 200, 113. A „növekvő” sorrend 002, 030, 111, 113, 140, 200, 201. Az f ennek megfelelő felírása a következő:

$$x_3^2 - 3x_2^3 + -x_1 x_2 x_3 + x_1 x_2 x_3^3 + x_1 x_2^4 + 2x_1^2 - i x_1^2 x_3 \,.$$

Az általános szabály tehát az, hogy először az első „jegyeket” kell sorba rakni, azután a második jegyeket, és így tovább. Hasonló elv szerint rendezzük egy lexikonban a címszavakat is (ábécé sorrendben), és ezért ennek a sorrendnek *lexikografikus rendezés* a neve.

2.6.3. Definíció. Legyenek r és s nem nulla elemei az R szokásos gyűrűnek. Azt mondjuk, hogy a

$$P = r x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n} \qquad \text{és} \qquad Q = s x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

tagok közül az első lexikografikusan megelőzi a másodikat, ha az első olyan j indexnél, ahol az $(m_1, \dots, m_n)$ és $(k_1, \dots, k_n)$ sorozatok eltérnek, $m_j < k_j$ teljesül. Másképp fogalmazva: van olyan $1 \le j \le n$, hogy $m_1 = k_1, m_2 = k_2, \dots, m_{j-1} = k_{j-1}$, de $m_j < k_j$. Erre a fogalomra a $P \prec Q$ jelölést fogjuk használni. Azt is írjuk majd, hogy $P \preceq Q$, ha $P \prec Q$, vagy P és Q az együtthatójuktól eltekintve megegyezik (vagyis a kitevősorozatuk ugyanaz).

A lexikografikus rendezés szoros kapcsolatban van azzal, ahogy polinomjainkat indukcióval definiáltuk. A kapcsolatot a következő gyakorlat írja le. Ez az összefüggés magyarázza, hogy a lexikografikus rendezést a fokszám valamiféle általánosításának, finomításának tekinthetjük.

2.6.2. Gyakorlat. Ha adott egy $f \in R[x_1, \dots, x_n]$ polinom, akkor rendezzük x_1 hatványai szerint (és írjuk is le a konstans taggal kezdve, fokszám szerint növekvő sorrendben). Az együtthatók $R[x_2, \dots, x_n]$ elemei lesznek, ezeket rendezzük x_2 hatványai szerint. A kapott együtthatókat x_3 hatványai szerint. És így tovább, végül „legbelül" x_n hatványai szerint rendezünk. Mutassuk meg, hogy ha a zárójeleket kibontjuk, de a sorrendet nem változtatjuk meg, akkor f tagjai lexikografikusan növekvő sorrendben lesznek.

Ha két egyhatározatlanú polinomot összeszorzunk, akkor a szorzat főtagja a két polinom főtagjainak szorzata lesz. Szeretnénk ezt az állítást többhatározatlanú polinomokra is általánosítani. Egy n-határozatlanú polinom (lexikografikus értelemben vett) *főtagján* a nem nulla tagjai közül azt értjük, ami a lexikografikus értelemben utolsó (néha mondjuk ezt úgy is, hogy „legnagyobb"). Például az imént vizsgált f polinom főtagja $-ix_1^2x_3$. A következő lemma segít meghatározni a szorzatpolinom főtagját.

2.6.4. Lemma. *Legyenek P', P, Q', Q egytagú, n-határozatlanú polinomok, melyeknek az együtthatója* 1. *Tegyük fel, hogy $P' \preceq P$ és $Q' \preceq Q$ teljesül. Ekkor $P'Q' \preceq PQ$. Ha itt egyenlőség áll, akkor $P' = P$ és $Q' = Q$.*

Bizonyítás. Legyen

$$P' = x_1^{m_1'} x_2^{m_2'} \dots x_n^{m_n'}, \quad P = x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}, \quad Q' = x_1^{k_1'} x_2^{k_2'} \dots x_n^{k_n'}, \quad Q = x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}.$$

Ekkor

$$P'Q' = x_1^{m_1'+k_1'} x_2^{m_2'+k_2'} \dots x_n^{m_n'+k_n'} \quad \text{és} \quad PQ = x_1^{m_1+k_1} x_2^{m_2+k_2} \dots x_n^{m_n+k_n}.$$

Arra vagyunk kíváncsiak, hogy hol tér el először ez a két kitevősorozat.

Nézzük meg először azt az egyszerű esetet, amikor $P' = P$. Ha $Q' = Q$, akkor nyilván $P'Q' = PQ$. Ha $Q' \ne Q$, akkor jelölje j azt az indexet, ahol Q' és Q kitevősorozata először eltér: $k_i' = k_i$ ha $i < j$, de $Q' \prec Q$ miatt $k_j' < k_j$. Tudjuk, hogy $P' = P$, ezért minden i-re $m_i' = m_i$. Tehát a $P'Q'$ és a PQ kitevősorozata is a j-edik helyen tér el először: $m_i' + k_i' = m_i + k_i$ ha $i < j$, viszont $m_j' + k_j' < m_j + k_j$. Ezért $P'Q' \prec PQ$.

Ha az előző bekezdés gondolatmenetében felcseréljük P-t Q-val és P'-t Q'-vel, akkor az adódik, hogy $P' \prec P$ és $Q' = Q$ esetén is $P'Q' \prec PQ$. Tehát már csak akkor kell bizonyítanunk az állítást, amikor $P' \prec P$ és $Q' \prec Q$.

Ebben az esetben azt állítjuk, hogy $P'Q'$ és PQ kitevősorozata ott fog először eltérni, ahol előbb van eltérés P és P' illetve Q és Q' sorozata között. Valóban, legyen j az az index, ahol P sorozata először eltér P' sorozatától, és ℓ az az index, ahol Q' sorozata először eltér Q sorozatától. Feltehetjük, hogy $j \leq \ell$ (vagyis hogy P' előbb kezd eltérni P-től, mint Q' a Q-tól), hiszen ellenkező esetben megcserélhetjük P-t Q-val és P'-t Q'-vel. Nyilván $i < j$ esetén $m'_i = m_i$ és $k'_i = k_i$, tehát ilyenkor $m'_i + k'_i = m_i + k_i$. Mivel $P' \prec P$, tudjuk, hogy $m'_j < m_j$. Ugyanakkor $j < \ell$ esetén $k'_j = k_j$, ha pedig $j = \ell$, akkor $k'_j < k_j$. Mindkét esetben azt kapjuk, hogy $m'_j + k'_j < m_j + k_j$. Tehát tényleg $P'Q' \prec PQ$. □

2.6.5. Következmény. *Ha R nullosztómentes, és $f, g \in R[x_1, \ldots x_n]$, akkor fg főtagja az f és g főtagjainak szorzata. Így $R[x_1, \ldots x_n]$ nullosztómentes.*

Bizonyítás. Legyen az f főtagja rP és a g főtagja sQ, ahol r és s az R gyűrű nem nulla elemei. Amikor f-et és g-t összeszorozzuk, akkor f egy tetszőleges $r'P'$ tagját megszorozzuk g egy tetszőleges $s'Q'$ tagjával, majd összevonjuk azokat a tagokat, amelyek csak az együtthatójukban különböznek. Nyilván $P' \preceq P$ és $Q' \preceq Q$. Az előző lemma szerint $P'Q' \preceq PQ$, vagyis a szorzatpolinomban $rsPQ$-nál lexikografikusan nagyobb tag nem keletkezhet. Azt kell még megnéznünk, hogy az összevonások során nem eshet-e ki az $rsPQ$ tag. A lemma szerint azonban $P'Q' \prec PQ$, kivéve ha $P' = P$ és $Q' = Q$. Ezért $rsPQ$ semmivel sem vonható össze, és így nem is tud kiesni. Az R nullosztómentessége miatt $rs \neq 0$, és így fg főtagja tényleg f és g főtagjainak szorzata. □

A főtagok az összeadásra is hasonlóan viselkednek, mint az egyváltozós polinomoknál. Ha két polinom főtagja nemcsak együtthatójában tér el, akkor összegüknek a főtagja a két főtag közül a lexikografikus értelemben nagyobbik lesz. Ha viszont a két főtag csak az együtthatóban tér el, akkor az összeg főtagját ezekből összevonással kapjuk, kivéve, ha ez a tag kiesik, ilyenkor a főtag lexikografikusan csökken, sőt akár a nullapolinom is lehet az eredmény (aminek nincs is főtagja).

Gyakorlatok, feladatok

2.6.3. Gyakorlat. Az alábbi $p(x_1, x_2, x_3, x_4)$ polinomot bontsuk fel homogén polinomok összegére, ezeket rendezzük lexikografikusan, és állapítsuk meg a p^7 polinomban egyrészt a lexikografikusan legnagyobb tagot, másrészt a legnagyobb fokú tagok közül a lexikografikusan legnagyobb tagot.

$$ix_1x_2x_3x_4^2 - x_1^2x_3^3 + 3x_1^3x_2 + \pi x_1^2x_2^3 + x_4 - x_1^2x_2^2x_3 + 2x_1^2x_2x_3x_4 - 6x_1^2x_2^2x_4\,.$$

2.6.4. Gyakorlat. Definiáljuk precízen egy n-változós polinomhoz tartozó n-változós polinomfüggvény fogalmát.

2.6.5. Feladat. Általánosítsuk az interpolációt többhatározatlanú polinomokra. Mutassuk meg, hogy véges test esetében minden véges sok változós függvény polinomfüggvény.

2.7. Szimmetrikus polinomok

Gyakran előfordul, hogy egy többhatározatlanú polinom *szimmetrikus.* Ilyen például a háromváltozós

$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + x_1 + x_2 + x_3 - x_1x_2x_3$$

polinom. Ebben a három határozatlan szerepe teljesen egyenrangú: ha például x_2-t és x_3-at kicseréljük, a polinom változatlan marad. Ugyanakkor

$$x_1^2x_2 + x_2^2x_3 + x_3^2x_1$$

nem szimmetrikus, mert például x_1 és x_2 cseréjekor a következőbe megy át:

$$x_2^2x_1 + x_1^2x_3 + x_3^2x_2\,,$$

ami nem az eredeti polinom, hiszen ebben például $x_1^2x_2$ nem szerepel.

2.7.1. Definíció. Az $f \in R[x_1, \ldots, x_n]$ polinomot szimmetrikus polinomnak nevezzük, ha bármely két határozatlant kicserélve a polinom önmagába megy át.

Nyilván szimmetrikus polinomok összege, különbsége és szorzata is szimmetrikus, és így a szimmetrikus polinomok részgyűrűt alkotnak a polinomok között. A gyökök és együtthatók összefüggésében (a 2.5.4. Tételben) szereplő σ_k kifejezések is szimmetrikus polinomok.

2.7.2. Definíció. Az $x_1, \ldots, x_n$ határozatlanú, k-adik *elemi szimmetrikus polinom* úgy keletkezik, hogy az $x_1, \ldots, x_n$ közül az összes lehetséges módon kiválasztunk k darabot, a kiválasztott x_i-ket összeszorozzuk, majd a kapott szorzatokat összeadjuk. E polinom jele $\sigma_k(x_1, \ldots, x_n)$, ahol $1 \leq k \leq n$. A σ_0 polinomot konstans 1-nek definiáljuk. (Néha használják $k > n$ esetén a $\sigma_k = 0$ konvenciót is).

Az elemi szimmetrikus polinomok azért fontosak, mert segítségükkel az összes többi szimmetrikus polinomot ki lehet fejezni, méghozzá egyértelműen. (Ezt illusztrálja például a 2.5.9. Gyakorlat.) De mit értünk azalatt, hogy „ki lehet fejezni”? Milyen műveleteket használhatunk eközben? Milyen értelemben egyértelmű ez a „kifejezés”? Vizsgáljunk meg először egy konkrét példát. Legyen

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - ix_1x_2x_3\,.$$

A 2.5.8. Feladat megoldásakor rájöttünk, hogy a négyzetösszeggel hogyan érdemes bánni:

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)\,.$$

Itt már csupa elemi szimmetrikus polinom szerepel. Tehát végülis

$$f = \sigma_1^2 - 2\sigma_2 - i\sigma_3\,.$$

Azaz f kifejezésekor összeadást, kivonást, szorzást, és f együtthatóit használtuk fel.

De polinomnak pontosan azokat a kifejezéseket neveztük, amelyek az említett három művelet használatakor keletkeznek. Vagyis azt mondhatjuk, hogy f-et az elemi szimmetrikus polinomok *polinomjaként* írtuk fel. Valóban, ha

$$F(y_1, y_2, y_3) = y_1^2 - 2y_2 - iy_3 \in \mathbb{C}[y_1, y_2, y_3]\,,$$

akkor a fenti képlet szerint

$$f = F(\sigma_1, \sigma_2, \sigma_3)\,,$$

(az egyenlőséget úgy kell érteni, hogy a két oldal, mint x_1, x_2, x_3 polinomja, megegyezik). Most már nem lehet gondunk az egyértelműség megfogalmazása sem: arról van szó, hogy $f(x_1, x_2, x_3)$ az $F(y_1, y_2, y_3)$ polinomot egyértelműen meghatározza.

2.7.3. Tétel [A szimmetrikus polinomok alaptétele]. *Legyen R szokásos gyűrű. Ekkor minden $f \in R[x_1, \ldots, x_n]$ szimmetrikus polinom egyértelműen felírható az elemi szimmetrikus polinomok polinomjaként. Ez azt jelenti, hogy létezik pontosan egy $F \in R[y_1, \ldots, y_n]$ polinom, melyre*

$$f = F(\sigma_1, \ldots, \sigma_n)\,.$$

A F együtthatói a f együtthatóiból összeadás és kivonás segítségével kaphatók.

Bizonyítás. Egyben eljárást is fogunk adni arra, hogy egy konkrét polinomot hogyan fejezzünk ki az elemi szimmetrikus polinomokkal.

2.7.1. Gyakorlat. Mutassuk meg, hogy ha az

$$ry_1^{k_1} y_2^{k_2} \ldots y_n^{k_n} \in R[y_1, \ldots, y_n]$$

polinomban az y_i helyére a $\sigma_i(x_1, \ldots, x_n)$ elemi szimmetrikus polinomot helyettesítjük, akkor

$$rx_1^{k_1+\cdots+k_n} x_2^{k_2+\cdots+k_n} \ldots x_{n-1}^{k_{n-1}+k_n} x_n^{k_n}$$

lesz az eredmény főtagja.

Látjuk, hogy a kapott főtagban a kitevők sorozata csökkenő. Ez nem véletlen, hanem így van minden szimmetrikus polinomban.

2.7.2. Gyakorlat. Mutassuk meg, hogy ha az $f \in R[x_1, \ldots, x_n]$ szimmetrikus polinom főtagja

$$rx_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}\,,$$

akkor $m_1 \geq m_2 \geq \cdots \geq m_n$, és f minden tagjában mindegyik határozatlan kitevője legfeljebb m_1 lehet. Igazoljuk, hogy az f polinomnak legfeljebb $(m_1 + 1)^n$ tagja lehet.

Legyen hát adva egy $f \in R[x_1, \ldots, x_n]$ szimmetrikus polinom. Le szeretnénk vonni belőle egy

$$g = s\sigma_1^{k_1} \sigma_2^{k_2} \ldots \sigma_n^{k_n}$$

alakú polinomot úgy, hogy a főtagja kiessen, de ne is termelődjön közben az eredeti főtagnál lexikografikusan nagyobb tag. Ha f főtagja $rx_1^{m_1}x_2^{m_2}\dots x_n^{m_n}$, akkor az előző két gyakorlat szerint, ha s-et r-nek választjuk, a k_i számokat pedig úgy, hogy

$$k_1+\dots+k_n=m_1\,,\quad k_2+\dots+k_n=m_2\,,\quad \dots\,,\quad k_{n-1}+k_n=m_{n-1}\,,\quad k_n=m_n$$

legyen, akkor f és g főtagja meg fog egyezni. Mivel $m_1\ge m_2\ge\dots\ge m_n$, a k_i számokat meg is lehet így választani, a következőképpen:

$$k_1=m_1-m_2\,,\quad k_2=m_2-m_3\,,\quad \dots\,,\quad k_{n-1}=m_n-m_{n-1}\,,\quad k_n=m_n\,.$$

Az $f-g$ szintén szimmetrikus polinom. Ha nulla, akkor készen vagyunk, hiszen g már az elemi szimmetrikus polinomok polinomja. Ha nem, akkor is tudjuk, hogy $f-g$ főtagja már lexikografikusan kisebb, mint f eredeti főtagja volt. Abban reménykedünk, hogy ezt az eljárást ismételgetve véges sok lépésben már a nulla polinomhoz jutunk, ami azt jelenti, hogy az eredeti polinomot felírtuk az elemi szimmetrikus polinomok polinomjaként.

A fenti 2.7.2. Gyakorlat mutatja, hogy az eljárás során soha nem fog m_1-nél nagyobb kitevő előfordulni. Vagyis mindegyik kitevő m_1+1-féle lehet: $0,1,\dots,m_1$ valamelyike. Ezért az eljárás során keletkező főtagból sem lehet több, mint $(m_1+1)^n$, azaz csak véges sok. Az eljárás tehát tényleg véges sok lépésben véget ér.

Most rátérünk az egyértelműség bizonyítására. Tegyük fel, hogy $F,G\in R[y_1,\dots,y_n]$, és $F(\sigma_1,\dots,\sigma_n)=G(\sigma_1,\dots,\sigma_n)$ (mint $x_1,\dots,x_n$ polinomjai). Meg kell mutatnunk, hogy $F=G$. Ha H jelöli az $F-G$ különbséget, akkor $H(\sigma_1,\dots,\sigma_n)=0$, és be kell látni, hogy $H=0$. Tegyük fel, hogy $H\ne0$, meg kell keresnünk a $H(\sigma_1,\dots,\sigma_n)$ egy olyan tagját, ami nem tud kiesni, ha a helyettesítés után az összevonásokat elvégezzük.

Ha $ry_1^{k_1}y_2^{k_2}\dots y_n^{k_n}$ egy tagja H-nak, akkor ebből a σ_i-k behelyettesítése után sok tag keletkezik, amelyek közül

$$P=rx_1^{k_1+\dots+k_n}x_2^{k_2+\dots+k_n}\dots x_{n-1}^{k_{n-1}+k_n}x_n^{k_n}$$

a lexikografikusan legnagyobb. A P-t kiejthetik a H egy másik tagjából keletkező tagok, hacsak nem érjük el, hogy azok mind lexikografikusan kisebbek legyenek, mint P. Hogyan kell ehhez a $k_1,\dots,k_n$ kitevőket választani?

Elsőnek H minden $ry_1^{k_1}y_2^{k_2}\dots y_n^{k_n}$ tagjához készítsük el a $k_1+\dots+k_n$ összeget, a legnagyobb ilyet jelölje m_1. Dobjuk ki H összes olyan tagját, amiben $k_1+\dots+k_n<m_1$. A megmaradó tagok mindegyikére számítsuk ki a $k_2+\dots+k_n$ összeget, és a legnagyobb ilyet jelöljük m_2-vel. Dobjuk ki most azokat a tagokat is, ahol $k_2+\dots+k_n<m_2$. Folytassuk az eljárást. Az utolsó lépésben a megmaradó tagok közül azokat nézzük, amelyekre k_n a legnagyobb, ez a legnagyobb érték legyen m_n. Azt állítjuk, hogy H-nak csak egyetlen olyan tagja marad, ahol $k_n=m_n$ is teljesül.

Tegyük fel ugyanis, hogy a megmaradt két ilyen tag is: $ry_1^{k_1}y_2^{k_2}\dots y_n^{k_n}$ és $r'y_1^{k'_1}y_2^{k'_2}\dots y_n^{k'_n}$. Ekkor tudjuk, hogy $k_n=m_n=k'_n$. Továbbá $k_{n-1}+k_n=m_{n-1}=k'_{n-1}+k'_n$, tehát $k_{n-1}=m_{n-1}-m_n=k'_n$. És így tovább, végül $k_1+\dots+k_n=m_1=k'_1+\dots+k'_n$ miatt

$k_1 = m_2 - m_1 = k_1'$. De ekkor H-nak ez a két tagja ugyanaz, hiszen az összes kitevőjük megegyezik.

Kijelöltük tehát H egy egyértelműen meghatározott $r y_1^{k_1} y_2^{k_2} \dots y_n^{k_n}$ tagját, aminek az a tulajdonsága, hogy $r\sigma_1^{k_1}\sigma_2^{k_2}\dots\sigma_n^{k_n}$ főtagja lexikografikusan nagyobb, mint a H bármely más tagjából a σ_i-k behelyettesítéskor keletkező bármelyik tag. Ezért ez a főtag nem eshet ki. Ezzel a szimmetrikus polinomok alaptételének a bizonyítását befejeztük. □

Az alaptétel szerint az

$$s_k(x_1, \dots, x_n) = x_1^k + x_2^k + \dots + x_n^k \qquad (k \geq 0)$$

hatványösszegeket is ki lehet fejezni a szimmetrikus polinomokkal. Erre nem mutatunk explicit képlet, hanem csak egy olyan összefüggést, amiből az $s_1, s_2, s_3, \dots$ hatványösszegeket sorra ki lehet számítani.

2.7.4. Tétel [Newton-Girard formulák]. *Az $s_k = s_k(x_1, \dots, x_n)$ és $\sigma_k = \sigma_k(x_1, \dots, x_n)$ polinomokra $k \geq n$ esetén*

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} - + \dots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0\,,$$

ha viszont $k \leq n$, akkor

$$s_k - \sigma_1 s_{k-1} + \sigma_2 s_{k-2} - + \dots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0\,.$$

Bizonyítás. Az elemi szimmetrikus polinomokat definiáló

$$(x - x_1)\dots(x - x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - + \dots + (-1)^n \sigma_n$$

azonosságba helyettesítünk x helyére x_j-t. Ekkor a baloldalon nullát kapunk, ezért

$$x_j^n - \sigma_1 x_j^{n-1} + \sigma_2 x_j^{n-2} - + \dots + (-1)^n \sigma_n = 0\,.$$

Szorozzuk ezt meg x_j^{k-n}-nel, és adjuk össze a kapott azonosságokat a $j = 1, 2, \dots, n$ értékekre. Ekkor az első Newton-Girard formulát kapjuk.

A második formulát n szerinti indukcióval bizonyítjuk be, $n = k$-tól elindulva. Ha $n = k$, akkor a második formula ugyanaz, mint az első (tehát igaz). Az indukció során feltesszük, hogy az állítás igaz $n - 1$-re (ahol $n - 1 \geq k$), és belátjuk, hogy n-re is igaz.

2.7.5. Lemma. *Tegyük fel, hogy az $f \in R[x_1, \dots, x_n]$ polinomban nincs olyan tag, amelyben mindegyik határozatlan előfordul. Ha f-re teljesül az, hogy bármelyik határozatlan helyébe nullát helyettesítve f-ből a nullapolinom lesz, akkor f maga is a nullapolinom.*

A lemma állítása nyilvánvaló, hiszen ha f-nek lenne egy nem nulla tagja, akkor a feltétel szerint ebben nem szerepel valamelyik x_j határozatlan, tehát ez a tag megmarad akkor is, amikor x_j helyébe írunk nullát. A lemmát alkalmazzuk a második Newton-Girard formula baloldalán álló polinomra. Mivel ez homogén k-adfokú, egyetlen tagban sem szerepelhet mindegyik változó (hiszen $k < n$). Helyettesítsünk az x_n változó helyébe nullát. Ekkor $s_j(x_1, \dots x_n)$-ből $s_j(x_1, \dots x_{n-1})$ lesz, $\sigma_j(x_1, \dots x_n)$-ből pedig $\sigma_j(x_1, \dots x_{n-1})$. Vagyis a

Newton-Girard formula eggyel kevesebb változós alakját kapjuk, amiről az indukciós feltevés miatt tudjuk, hogy igaz. Ugyanez történik akkor is, ha x_n helyett egy másik változó helyébe írunk nullát, hiszen polinomjaink szimmetrikusak. A lemma feltételei tehát teljesülnek, ami a második Newton-Girard formulát bizonyítja. □

Ez a gondolatmenet megmagyarázza azt is, hogy miért a k szám szerepel a második Newton-Girard formula végén: a $k = n$ esetben ez öröklődik az első formulából, utána pedig n növelésével nem változik meg.

Gyakorlatok, feladatok

2.7.3. Gyakorlat. Igaz-e, hogy szimmetrikus polinom minden homogén komponense is szimmetrikus?

2.7.4. Gyakorlat. Egy 3-határozatlanú szimmetrikus polinom lexikografikusan legnagyobb tagja $x_1^2x_2^2x_3$. Lehet-e neki tagja $x_1x_2^3x_3$? Szerepelhet-e hatodfokú tag? Hány tag lehet legfeljebb? Amikor elemi szimmetrikusakkal írjuk fel, mi az eljárás első lépése?

2.7.5. Gyakorlat. A 2.6.3. Gyakorlatban szereplő p polinomban helyettesítsük be mindegyik x_i helyére a négy határozatlanú σ_i elemi szimmetrikus polinomot, és adjuk meg az eredménynek egy olyan tagját, amelynek nem nulla az együtthatója.

2.7.6. Gyakorlat. Írjuk fel az elemi szimmetrikus polinomok polinomjaként az alábbi polinomot:

$$f(x_1, \ldots, x_n) = \sum_{1 \le i \ne j \le n} x_i^2 x_j \,.$$

2.7.7. Gyakorlat. Határozzuk meg az $x^n + x + 1$ polinom (komplex) gyökeinek köbösszegét, és a gyökök reciprokainak összegét ($n \ge 2$).

2.7.8. Gyakorlat. Legyenek a, b, c az $x^3 + 3x + 1$ polinom gyökei. Írjuk fel azt a harmadfokú normált polinomot, melynek gyökei a^2, b^2, c^2, illetve $a + b, a + c, b + c$.

2.7.9. Feladat. Legyen $f \in R[x_1, \ldots, x_n]$ egy homogén k-adfokú szimmetrikus polinom, melyben minden határozatlan legfeljebb az m-edik hatványon szerepel. Mutassuk meg, hogy ha $\sigma_1^{k_1} \ldots \sigma_n^{k_n}$ nem nulla együtthatóval szerepel az f-nek az elemi szimmetrikus polinomokkal való felírásában, akkor

$$k_1 + k_2 + \cdots + k_n \le m \,,$$
$$k_1 + 2k_2 + \cdots + nk_n = k \,.$$

Hogyan segítenek ezek a képletek az f polinom elemi szimmetrikus polinomokkal való előállításában?

2.8. Összefoglaló

A komplex együtthatós polinomok olyan formális kifejezések, amelyek határozatlanokból („ismeretlenekből", „változókból"), és komplex számokból keletkeznek összeadás, kivonás és szorzás felhasználásával. Egy határozatlan esetén minden polinom a zárójelek kibontásával $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ alakra hozható. Két ilyen alakban felírt polinom akkor *egyenlő,* ha a megfelelő együtthatóik megegyeznek (2.1.1. Definíció). Definiáltuk polinomok összegét és szorzatát, amelyek a szokásos számolási szabályoknak tettek eleget (2.1.4. Állítás). Bevezettük a polinom *fokának* a fogalmát, és megmutattuk, hogy az összeg foka legfeljebb a tagok fokainak maximuma lehet (2.1.2. Állítás), szorzat foka pedig a tényezők fokainak összege, és ezért a polinomok szorzása nullosztómentes (2.1.2. Állítás). Ebből levezettük, hogy a komplex együtthatós polinomok között csak a nem nulla konstans polinomoknak létezik inverze (2.1.5. Állítás).

Felmerült az igény, hogy egy polinom együtthatói ne csak számok, hanem például mod m maradékok, vagy (a többhatározatlanú polinomok kényelmes bevezetéséhez) akár polinomok is lehessenek, szóval mindenféle, amivel a „szokásos szabályok szerint" számolni szoktunk. Ezért definiáltuk a kétváltozós művelet általános fogalmát, és több fontos tulajdonságát (asszociativitás, kommutativitás, neutrális elem, inverz, hatvány és többszörös: 2.2.1, 2.2.2, 2.2.3, 2.2.8. Definíciók). Ezekből a tulajdonságokból felépítettük a félcsoport, a *csoport,* a *gyűrű* és a *test* fogalmát (2.2.4, 2.2.5, 2.2.9, 2.2.10. Definíciók). Megemlítettük a részstruktúrák (részcsoport, részgyűrű) fogalmát is. Bevezettük a nullosztó fogalmát általános gyűrűben (2.2.13. Definíció), és megmutattuk, hogy minden ferdetest nullosztómentes (2.2.14. Tétel). Szokásos gyűrűnek neveztük a kommutatív egységelemes, nullosztómentes gyűrűket, mert ezek azok, ahol az összeadás, kivonás, szorzás a „szokásos" tulajdonságokkal rendelkezik. Bevezettük a művelettartó leképezés általános fogalmát (2.2.17. Definíció).

A 2.3. Szakaszban megmutattuk, hogy egy kommutatív, egységelemes gyűrű felett hogyan értelmezhetünk polinomokat, és megállapítottuk, hogy ha a gyűrű nullosztómentes is, akkor általában is igazak maradnak a komplex együtthatós polinomokra megismert alaptulajdonságok. A 1.6. Szakasz mintájára a polinomok precíz bevezetésének egy módjáról is szó esett.

Egy R gyűrű feletti polinom esetében definiáltuk, hogy hogyan lehet behelyettesíteni az R gyűrű elemeit, és bevezettük a *gyök* és a *gyöktényező* fogalmát (2.4.3. Definíció). A Horner-elrendezés lehetővé tette az elemek gyors behelyettesítését, és a gyöktényezők kiemelését (2.4.4. Állítás). Megmutattuk, hogy nullosztómentes gyűrű felett a gyöktényezők egyszerre is kiemelhetők, és ezért *egy polinomnak legfeljebb annyi gyöke lehet, mint a foka* (2.4.5. Tétel). Ebből adódott a polinomok azonossági tétele (2.4.6. Következmény), amely szerint ha két polinom több helyen megegyezik, mint a fokuk, akkor a két polinom (együtthatóról együtthatóra) egyenlő. Bevezettük a *polinomfüggvény* fogalmát (2.4.1. Definíció), és megmutattuk, hogy végtelen gyűrű felett ez meghatározza a polinomot, de véges gyűrű felett nem. Röviden szót ejtettünk a Lagrange- és Newton-interpolációról is.

Ha egy polinomból az összes gyöktényezőt kiemelve csak egy konstans marad (ez szükségképpen a polinom főegyütthatója lesz), akkor azt mondjuk, hogy a polinomot *gyöktényezős alakra* bontottuk. Ez mindig bekövetkezik úgynevezett *algebrailag zárt* alaptest esetén, ezek azok a testek, amelyekben minden nem konstans polinomnak van gyöke (2.5.1. Definíció). Speciálisan a komplex számok teste is algebrailag zárt, ez az algebra alaptétele (2.5.2. Tétel), amelyet egyelőre nem tudtunk bebizonyítani. Bevezettük a gyök multiplicitásának, azaz a *többszörös gyöknek* a fogalmát (2.5.3. Definíció). A gyöktényezős alak beszorzásával kaptuk *a gyökök és együtthatók közötti összefüggéseket* (2.5.4. Tétel, 2.5.5. Következmény).

A *többhatározatlanú polinomokat* indukcióval olyan egyhatározatlanú polinomként definiáltuk, amelyek együtthatói eggyel kevesebb határozatlanú polinomok (2.6.1. Definíció). Nullosztómentes gyűrű felett ezek is nullosztómentes gyűrűt alkotnak, melynek invertálható elemei az invertálható konstans polinomok lesznek. Definiáltuk többhatározatlanú polinom fokát, és a homogén polinomokat. Bevezettük egy polinom tagjainak *lexikografikus rendezését* (2.6.3. Definíció). Megmutattuk, hogy nullosztómentes gyűrű felett két polinom szorzatának lexikografikusan legnagyobb tagja (azaz főtagja) a két tényező főtagjainak szorzata (2.6.5. Következmény).

Egy polinomot *szimmetrikusnak* nevezünk, ha bármely két határozatlan cseréjekor önmagába megy át. Ilyenek a gyökök és együtthatók összefüggéseiből kapott elemi szimmetrikus polinomok (2.7.2. Definíció). Beláttuk a *szimmetrikus polinomok alaptételét,* mely szerint minden szimmetrikus polinom egyértelműen felírható az elemi szimmetrikus polinomok polinomjaként (2.7.3. Tétel). Végül levezettük a hatványösszegeket az elemi szimmetrikus polinomokból rekurzívan előállító Newton-Girard formulákat (2.7.4. Tétel).

3. A POLINOMOK SZÁMELMÉLETE

Ha van két nem egyenlő számunk, a kisebbet váltakozva mindig kivonjuk a nagyobból, és a maradék sosem osztja a megelőző számot, míg csak nem az egység a maradék, akkor az eredeti számok relatív prímek.

Euklidész: *Elemek*
(Mayer Gyula fordítása)

Könyvünk eddigi részében lényegében csak középiskolai ismeretekre támaszkodtunk. Ez most sem változik meg, de a polinomok számelméletének tárgyalásakor nagyon hasznos, ha az olvasó már rendelkezik néhány alapvető ismerettel az egész számok számelméletéről. Ezek az ismeretek megszerezhetők például Freud Róbert és Gyarmati Edit [**4**] könyvének első fejezetéből. Konkrétan érdemes átvenni az oszthatóság alaptulajdonságait, az egység fogalmát, a legnagyobb közös osztó definícióját és meghatározását az euklideszi algoritmussal, a felbonthatatlan és prímszám közötti különbséget, és végül a számelmélet alaptételét, bizonyítással együtt.

3.1. Számelméleti alapfogalmak

Az egész számok között a számelmélet alaptétele teszi lehetővé, hogy egy szám szorzatra bontásait áttekintsük. Ugyanígy fontos tudnunk azt is, hogy polinomokat hogyan lehet szorzattá bontani. Például x^2+1 a komplex együtthatós polinomok között felbontható:

$$x^2+1=(x+i)(x-i)\,.$$

Vizsgáljuk meg, hogyan bontható föl a valós együtthatós polinomok között. Ha

$$x^2+1=f(x)g(x)\,,$$

akkor f és g fokainak összege kettő. Ha f elsőfokú lenne, azaz $f(x)=ax+b$, ahol $a\neq 0$, akkor a valós $-b/a$ szám gyöke lenne x^2+1-nek, ami lehetetlen. Ezért a fenti felbontásban f és g egyike konstans polinom kell, hogy legyen. Tehát csak olyasféle felbontás létezik, mint például

$$x^2+1=(2/3)\big((3/2)x^2+(3/2)\big)\,.$$

Ez a felbontás nem érdekes, hiszen nem mond semmi újat az x^2+1 polinomról. Példánk azt mutatja, hogy $\mathbb{C}[x]$ és $\mathbb{R}[x]$ „számelmélete" másmilyen, vagyis minden egyes R gyűrű esetében az $R[x]$ polinomgyűrűt külön kell megvizsgálni számelméleti szempontból.

3.1.1. Gyakorlat. Határozzuk meg az x^2-2 polinom összes lehetséges felbontásait a valós együtthatós, illetve a racionális együtthatós polinomok gyűrűjében.

3.1.2. Gyakorlat. Határozzuk meg az x^2+1 polinom felbontásait $\mathbb{Z}_2[x]$-ben és $\mathbb{Z}_3[x]$-ben.

Számelméleti kérdéseket nem csak az egész számok és a polinomok között érdemes vizsgálni. Például az úgynevezett *Gauss-egészek* az $a+bi$ alakú komplex számok, ahol a és b egészek (2.2.15. (2) Gyakorlat). Ezek között is érvényes a számelmélet alaptételének megfelelő állítás, és ennek felhasználásával érdekes egész számokra vonatkozó problémákat oldhatunk meg (például kideríthetjük, mely egész számok állnak elő két négyzetszám összegeként).

Ha ilyen sokféle gyűrűben kell számelmélettel foglalkozni, akkor az a gazdaságos hozzáállás, ha a fogalmakat egy általános gyűrűben definiáljuk, és általános tételeket bizonyítunk. Az alábbiakban mindig az egész számok $\mathbb{Z}$ gyűrűjét tartsuk szem előtt főpéldaként.

3.1.1. Definíció. Legyen R kommutatív gyűrű. Azt mondjuk, hogy az $r \in R$ elem *osztja* az $s \in R$ elemet, ha van olyan $t \in R$, hogy $rt = s$. Az oszthatóság jele $r \mid s$. Azt, hogy $r \mid s$, úgy is mondjuk, hogy r *osztója* s-nek, illetve hogy s *többszöröse* r-nek.

Az áthúzott oszthatóság jel azt jelenti: nem osztható. Néha fontos feltüntetnünk a jelölésben is, hogy melyik gyűrűben értjük az oszthatóságot, ilyenkor $r \mid s$ helyett $r \mid_R s$-et írunk. Például $2 \nmid_{\mathbb{Z}} 3$, de $2 \mid_{\mathbb{Q}} 3$ (hiszen $2 \cdot (3/2) = 3$). Hasonlóképpen $2 \nmid_{\mathbb{Z}[x]} 3x+1$, de $2 \mid_{\mathbb{Q}[x]} 3x+1$.

3.1.3. Gyakorlat. Legyen R kommutatív gyűrű, és $r, s, t \in R$. Igazoljuk az alábbiakat.

(1) Ha $r \mid s$ és $r \mid t$, akkor $r \mid s \pm t$.
(2) Ha $r \mid s$, akkor $r \mid st$ (sőt $rt \mid st$).
(3) Ha $r \mid s$ és $s \mid t$, akkor $r \mid t$ (az oszthatóság *tranzitív*).
(4) Ha R egységelemes, akkor $r \mid r$ minden $r \in R$ esetén (az oszthatóság *reflexív*).

3.1.4. Gyakorlat. Igazoljuk, hogy a nulla csak a nullának osztója (azaz $0 \mid s \implies s = 0$), de minden elemnek többszöröse (azaz $r \mid 0$ minden $r \in R$ esetén). Egy testben mikor teljesül az $r \mid s$ oszthatóság?

3.1.5. Gyakorlat. Igazoljuk, hogy ha n egész szám, akkor egy $p \in \mathbb{Z}[x]$ polinom akkor és csak akkor osztható ($\mathbb{Z}[x]$-ben) n-nel, ha minden együtthatója osztható ($\mathbb{Z}$-ben) n-nel. Általánosítsuk a feladatot $\mathbb{Z}$ helyett tetszőleges R kommutatív, egységelemes gyűrűre.

Az egész számok között megszoktuk, hogy egy szám és ellentettje oszthatóság szempontjából ugyanúgy viselkedik. A valós együtthatós polinomok között azonban egy f polinom kétszerese (fele, sőt $\sqrt{2}$-szöröse, π-szerese) is ugyanúgy viselkedik, mint f. Valóban $f \mid 2f$ és $2f \mid f$ is igaz (utóbbi azért, mert az $1/2$ is valós szám), és így f-nek és $2f$-nek ugyanazok az osztói is, és a többszörösei is.

3.1.2. Definíció. Legyen R kommutatív gyűrű. Azt mondjuk, hogy az $r, s \in R$ elemek egymás *asszociáltjai*, ha egymás osztói (vagyis $r \mid s$ és $s \mid r$ is teljesül). Az asszociáltság jele $r \sim s$.

Az „asszociált” szó helyett tehát ezt is mondhatjuk: „oszthatóság szempontjából egyformán viselkedő, megkülönböztethetetlen”. Így szóba jönne a következő definíció is: r és s asszociáltak, ha tetszőleges $t \in R$ esetén $r \mid t$ és $s \mid t$ ugyanakkor teljesül (vagyis ha a két elemnek ugyanazok a többszöröseik). Így az asszociáltság nem egységelemes gyűrűben is reflexív lenne (vö. 3.1.21. Gyakorlat). Az olvasónak érdemes végiggondolnia, hogy egységelemes gyűrűben, ahol tehát minden elem osztója önmagának, az oszthatóság tranzitivitása miatt ez ugyanaz az asszociáltság-fogalom, mint ami a fenti 3.1.2. Definícióban szerepel.

3.1.6. Gyakorlat. Mutassuk meg, hogy ha R egységelemes, kommutatív gyűrű, akkor

(1) Minden $r \in R$ esetén $r \sim r$ (az asszociáltság *reflexív*).
(2) Ha $r \sim s$, akkor $s \sim r$ (az asszociáltság *szimmetrikus*).
(3) Ha $r \sim s$ és $s \sim t$, akkor $r \sim t$ (az asszociáltság *tranzitív*).

Tegyük fel, hogy r és s asszociáltak. Ekkor $re = s$ és $se' = s$ teljesül alkalmas $e, e' \in R$ elemekre. Innen $ree' = se' = r$. Ha R egységelemes és nullosztómentes, akkor $r \neq 0$ esetén r-rel egyszerűsíthetünk, és $ee' = 1$ adódik. Ezt úgy is fogalmazhatjuk, hogy $e \mid 1$.

3.1.3. Definíció. Legyen R kommutatív, egységelemes gyűrű. Azt mondjuk, hogy az $e \in R$ elem *egység*, ha az egységelemnek (vagyis az 1 elemnek) osztója.

Ne tévesszük össze tehát az egység és az egységelem fogalmát! Az egységelem az az $1 \in R$ elem, amelyre $1r = r1 = r$ teljesül minden $r \in R$ esetén. Az egységek ennek az osztói, vagyis az R invertálható elemei (lásd a 2.2.3. Definíciót). Az egységek tehát az $R^\times$ halmaznak, azaz R multiplikatív csoportjának az elemei. (Az „egység” és „invertálható” szavak kommutatív, egységelemes gyűrűben szinonimák, de számelméleti ízű vizsgálatokban inkább az egység szó használatos.) Például $\mathbb{Z}$ egységei 1 és -1.

Az R egy eleme tehát pontosan akkor egység, ha R minden elemének osztója. Azt gondolhatnánk, hogy érdemesebb az egységet így definiálni, mert akkor a fogalom nem egységelemes gyűrűben is értelmessé válna. Azonban a 3.1.21. Gyakorlat szerint nem egységelemes, de nullosztómentes gyűrűben nem lehetnek egységek ebben a kiterjesztett értelemben sem.

3.1.4. Állítás. *Tegyük fel, hogy R kommutatív, egységelemes, nullosztómentes (azaz szokásos) gyűrű. Ekkor tetszőleges $r \in R$ asszociáltjai pontosan az egységszeresei.*

Bizonyítás. A nulla asszociáltja nyilván csak a nulla lehet. Ha $r \neq 0$ és $s \in R$ asszociáltja r-nek, akkor az imént beláttuk, hogy s az r-nek egységszerese. Megfordítva, ha e egység, azaz $ee' = 1$ alkalmas e'-re, akkor r és re asszociáltak, hiszen $(re)e' = r$ miatt $re \mid r$. □

3.1.7. Gyakorlat. Igazoljuk, hogy $\mathbb{Z}[x]$ egységei az 1 és -1 konstans polinomok, $\mathbb{R}[x]$ egységei pedig a nem nulla konstans polinomok. Általában mutassuk meg, hogy ha R szokásos gyűrű, akkor $R[x]$ egységei pontosan R egységei lesznek (mint konstans polinomok). Speciálisan tehát test fölötti polinomgyűrű egységei a nem nulla konstans polinomok.

A következő célunk a számelmélet alaptételének megfelelő állítás megfogalmazása tetszőleges gyűrűben. Az egyszerűség és a jobb érthetőség kedvéért *mostantól a számelméleti vizsgálatok során feltesszük, hogy minden gyűrű kommutatív, nullosztómentes és egységelemes, azaz szokásos gyűrű.* (Néhány feladatban azért meg fogjuk vizsgálni, hogy ezek a feltevések mindig szükségesek-e.)

A számelmélet alaptétele durván fogalmazva azt mondja ki, hogy minden számot egyértelműen föl lehet bontani olyan számok szorzatára, amik tovább már nem bonthatók. A „tovább már nem bontható" szám fogalmát azonban pontosan definiálnunk kell, hiszen például a 7, amit az egész számok között „tovább már nem bonthatónak" gondolunk, igenis felbontható:

$$7 = 1 \cdot 7 = 7 \cdot 1 = (-1) \cdot (-7) = (-7) \cdot (-1)\,.$$

Azonban másféle felbontás nincs, ezek pedig ugyanúgy érdektelenek, mint ahogy a fenti példában érdektelen volt, amikor az $x^2 + 1$ polinomból kiemeltük a $2/3$-ot. Ezekben az „érdektelen" felbontásokban az a közös, hogy egy egységet emelünk ki, és ami megmarad, az az eredeti elemnek egy asszociáltja. Az ilyen felbontást triviálisnak nevezzük.

3.1.5. Definíció. Legyen R szokásos gyűrű, és $0 \neq r = bc$, ahol $r, b, c \in R$. Azt mondjuk, hogy az r elemnek ez a felbontása *triviális,* ha b és c egyike r-nek asszociáltja. Ami ezzel ekvivalens: b és c közül a másik egység.

Egy elem tehát akkor lesz „tovább már nem bontható", ha nincs nemtriviális felbontása (azaz ha van is felbontása, az csak triviális lehet). Ilyen tulajdonságú elem az 1 és a -1 is az egész számok között, de ezeket mégsem tekintjük építőkőnek akkor, ha egy általános számot akarunk minél jobban szétbontani. Ezért a most következő definícióban az egységeket is kizárjuk.

3.1.6. Definíció. Legyen R szokásos gyűrű. A $p \in R$ elemet *felbonthatatlannak* vagy *irreducibilisnek* nevezzük, ha nem nulla, nem egység, és p-nek nincs nemtriviális felbontása.

A fenti példák szerint a 7 szám felbonthatatlan $\mathbb{Z}$-ben, az $x^2 + 1$ polinom pedig felbonthatatlan, más szóval irreducibilis $\mathbb{R}[x]$-ben, de nem irreducibilis $\mathbb{C}[x]$-ben.

Az „irreducibilis" és „felbonthatatlan" szavak tehát ugyanazt jelentik. Ha a vizsgált gyűrű elemei számok (például egészek vagy Gauss-egészek), akkor szokásosabb a „felbonthatatlan" szót használni. Ha viszont egy $R[x]$ polinomgyűrűben dolgozunk, akkor inkább az „irreducibilis polinom" kifejezést használjuk. Ahelyett, hogy „f irreducibilis $R[x]$-ben" sokszor azt fogjuk mondani, hogy „f irreducibilis R *fölött*". Ha egy nem nulla és nem egység polinom nem irreducibilis, akkor *reducibilisnek* is hívjuk majd.

3.1.7. Definíció. Azt mondjuk, hogy az R gyűrűben érvényes a számelmélet alaptétele (azaz hogy R *alaptételes),* ha R minden nem nulla és nem egység eleme sorrendtől és asszociáltságtól eltekintve egyértelműen felírható R irreducibilis elemeinek szorzataként.

Külön is felhívjuk a figyelmet arra, hogy csak a nem nulla és nem egység elemeket akarjuk felbontani irreducibilisek szorzatára. Szokásos gyűrűben mást nem is lehet: a nulla

minden felbontásában lesz nulla tényező, ami nem irreducibilis, egy egység felbontásában pedig minden tényező egység lesz.

Most precízen megfogalmazzuk, mit is jelent a felbontás egyértelműsége. A 15 számot az egész számok között négyféleképpen bonthatjuk felbonthatatlanok szorzatára:

$$15 = 3 \cdot 5 = 5 \cdot 3 = (-3) \cdot (-5) = (-5) \cdot (-3) \,.$$

Az első felbontásból az utolsót úgy kapjuk meg, hogy megcseréljük a sorrendet, majd mindkét tényezőnek vesszük egy-egy asszociáltját. Ezt általánosítva a felbontás egyértelműsége a következőt jelenti. Bárhogy is vesszük az r elemnek két

$$r = p_1 \dots p_k = q_1 \dots q_\ell$$

felbontását irreducibilisek szorzatára, a tényezők száma ugyanannyi (tehát $k = \ell$), és a két felbontás tényezői egymással párba állíthatók úgy, hogy a párok tagjai egymás asszociáltjai legyenek. Ezt a párba állítást még formálisabban úgy fogalmazhatjuk, hogy létezik olyan g kölcsönösen egyértelmű megfeleltetése az $\{1, 2, \dots, k\}$ halmaznak önmagába úgy, hogy p_i és párja, azaz $q_{g(i)}$ asszociáltak.

Az egész számok alaptétel szerinti felbontásában össze szokás vonni az „egyforma" felbonthatatlanokat, ekkor kapjuk egy szám *kanonikus alakját.* A polinomok gyöktényezős alakjának vizsgálatakor is beszéltünk kanonikus alakról hasonló értelemben. Mi is lesz a -4 szám kanonikus alakja?

$$-4 = 2 \cdot (-2) = (-2) \cdot 2 = -2^2 = -(-2)^2 \,,$$

vagyis az asszociált felbonthatatlanokat csak úgy tudjuk összevonni, ha egy -1-es tényező is megmarad! Ezért a kanonikus alakban meg kell engednünk egy egység tényezőt is.

3.1.8. Definíció. Az $r \neq 0$ elem *kanonikus alakja*

$$r = e p_1^{\alpha_1} \dots p_m^{\alpha_m} \,,$$

ahol e egység, a p_i páronként nem asszociált felbonthatatlan elemek, az α_i pedig nemnegatív egész számok.

Kanonikus alakja az egységeknek is van, például a fenti képletben vehetjük az $m = 0$ értéket. Az elemi számelméletből tudjuk, hogy az α_i kitevőkről néha érdemes feltenni, hogy mindegyik pozitív (ez a helyzet például, ha az Euler-féle φ függvény képletét akarjuk alkalmazni), néha viszont célszerű megengedni a nulla kitevőket is (ha több szám kanonikus alakjában ugyanazokat a felbonthatatlan elemeket akarjuk szerepeltetni, például a legnagyobb közös osztó meghatározásakor).

3.1.8. Kérdés. A közönséges pozitív egész számok kanonikus alakjának vizsgálatakor a számelméletben miért nem szokás az egységtényezőről beszélni? Mely negatív egész számok felírásakor lehet elkerülni az egységtényezőt?

3.1.9. Gyakorlat. Fogalmazzuk meg pontosan, hogy milyen értelemben egyértelmű a kanonikus alak, és bizonyítsuk is be az állítást.

Ebben a fejezetben még nem foglalkozunk azzal a kérdéssel, hogy általános gyűrűben hogyan (és milyen feltételek mellett) lehet bebizonyítani a számelmélet alaptételét. Annyit azonban megteszünk, hogy röviden átismételjük azt az utat, ahogy az egész számok gyűrűjében az alaptétel bebizonyítható, mert ez elvezet bennünket néhány fontos fogalomhoz.

Az egész számok között megmutattuk, hogy elvégezhető a maradékos osztás, és ennek felhasználásával az euklideszi algoritmus, amellyel előállítható tetszőleges két a és b szám (a, b) *legnagyobb közös osztója.* Az euklideszi algoritmusból azt is láttuk, hogy (a, b) felírható $ax + by$ alakban, ahol a és b egész számok. Ebből levezettük, hogy az egész számok körében minden felbonthatatlan p elem *prímtulajdonságú,* azaz ha p osztója egy szorzatnak, akkor osztója valamelyik tényezőnek is. A prímtulajdonságból könnyen következik a számelmélet alaptételének egyértelműségi állítása. A felbontás létezésének bizonyításához azt használtuk fel, hogy ha egy számot nemtriviálisan szorzatra bontunk, akkor a tényezők (abszolút értékben) kisebbek, mint az eredeti szám (abszolút értéke).

A most szóba került fogalmak közül elsőként a legnagyobb közös osztót vizsgáljuk meg. Általános gyűrűben nem beszélhetünk arról, hogy az egyik gyűrűelem „nagyobb" lenne a másiknál. Szerencsére az egész számok esetében megtanultuk, hogy két szám legnagyobb közös osztója nemcsak nagyságra a legnagyobb a közös osztók között, hanem oszthatóság tekintetében is: a legnagyobb közös osztó ugyanis minden közös osztónak többszöröse. Ez a definíció már tetszőleges gyűrűre átvihető. Hogy ezt a különbséget hangsúlyozzuk, legnagyobb közös osztó helyett kitüntetett közös osztóról fogunk beszélni.

3.1.9. Definíció. Legyen R szokásos gyűrű és $r, s \in R$. Azt mondjuk, hogy egy $t \in R$ elem *kitüntetett közös osztója* r-nek és s-nek, ha t közös osztó (azaz $t \mid r$ és $t \mid s$), és t minden közös osztónak többszöröse (azaz ha $t' \mid r$ és $t' \mid s$, akkor $t' \mid t$). Az r és s *relatív prímek*, ha a kitüntetett közös osztójuk egység.

3.1.10. Gyakorlat. Mutassuk meg, hogy ha a kitüntetett közös osztó létezik, akkor asszociáltság erejéig egyértelműen meghatározott.

Ez az állítás lehetővé teszi, hogy jelölést vezessünk be a kitüntetett közös osztóra, ami ugyanúgy (r, s) lesz, ahogy egész számok esetében. Fontos észben tartanunk azonban, hogy ez az elem csak asszociáltság erejéig meghatározott. Az egész számok között ezt a problémát úgy oldottuk meg, hogy a legnagyobb közös osztónak mindig a nemnegatív értékét vettük. Hasonlóképpen test fölötti polinomok között néha szokás a kitüntetett közös osztónak azt az értékét venni, amely normált polinom. Általános gyűrűben ilyen egyszerűsítés nem lehetséges.

3.1.11. Gyakorlat. Legyen R alaptételes gyűrű.

(1) Mutassuk meg, hogy R bármely két elemének létezik „közös kanonikus alakja", amelyben ugyanazok a felbonthatatlanok szerepelnek, csak esetleg más (és esetleg nulla) kitevővel.
(2) Hogyan jellemezhetjük r és s közös kanonikus alakja segítségével azt, hogy r osztója s-nek?

(3) Mutassuk meg, hogy R bármely két elemének van kitüntetett közös osztója, és adjunk is rá képletet a két szám közös kanonikus alakja segítségével.
(4) Általánosítsuk a *kitüntetett közös többszörös* fogalmát is szokásos gyűrűre. Mutassuk meg, hogy ez asszociáltság erejéig egyértelmű, hogy alaptételes gyűrűben mindig létezik, és adjunk rá képletet a kanonikus alak segítségével.
(5) Hogyan kell módosítani a kapott képleteket, ha kettőnél több szám kitüntetett közös osztóját, illetve kitüntetett közös többszörösét akarjuk kiszámítani?

Az r és s elemek kitüntetett közös többszörösét $[r, s]$ fogja jelölni, ez az elem is csak asszociáltság erejéig meghatározott.

3.1.10. Definíció. Legyen R szokásos gyűrű és $p \in R$. Azt mondjuk, hogy p *prímtulajdonságú* (vagy egyszerűen csak prím), ha nem nulla, nem egység, és tetszőleges $r, s \in R$ esetén ha $p \mid rs$, akkor $p \mid r$ vagy $p \mid s$.

3.1.12. Gyakorlat. Mutassuk meg, hogy minden prímtulajdonságú elem felbonthatatlan, és ha R alaptételes, akkor minden felbonthatatlan eleme prím.

Most következő célunk az, hogy a legfontosabb polinomgyűrűkben bebizonyítsuk a számelmélet alaptételét, és hogy minél többet megtudjunk arról, mik az irreducibilis polinomok ezekben a gyűrűkben.

Gyakorlatok, feladatok

3.1.13. Gyakorlat. Igaz-e a $2x \mid 3x^2$ oszthatóság rendre a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ fölötti polinomok gyűrűjében?

3.1.14. Gyakorlat. Legyen R szokásos gyűrű, és $r \mid s$ két eleme. Mi lesz a kitüntetett közös osztójuk? Mi lesz r és 0 kitüntetett közös osztója?

3.1.15. Gyakorlat. Legyen R szokásos gyűrű. A nullának lehet benne nemtriviális felbontása? Prímtulajdonságú-e? Mi a helyzet az egységelemmel?

3.1.16. Gyakorlat. Igazoljuk, hogy ha R alaptételes gyűrű, akkor tetszőleges $r, s, t \in R$ esetén (rt, st) és $(r, s)t$ asszociáltak (ez *a kitüntetett közös osztó kiemelési tulajdonsága*). Vezessük le ezt a tulajdonságot akkor is, ha R alaptételessége helyett azt tudjuk, hogy tetszőleges r és s esetén (r, s) felírható $rx + sy$ alakban alkalmas $x, y \in R$ elemekre.

3.1.17. Gyakorlat. Legyen R szokásos gyűrű, amelyben bármely két elemnek van kitüntetett közös osztója, és erre érvényes a kitüntetett közös osztó kiemelési tulajdonsága.

(1) Mutassuk meg, hogy ha egy elem osztója egy szorzatnak, de relatív prím az egyik tényezőhöz, akkor osztója a másik tényezőnek. Képletben: ha $r \mid st$ és $(r, s) \sim 1$, akkor $r \mid t$.
(2) Igazoljuk, hogy R minden irreducibilis eleme prím.

3.1.18. Feladat. Legyen R szokásos gyűrű, amelyben mindegyik irreducibilis elem prím. Mutassuk meg, hogy R-ben érvényes a számelmélet alaptételének egyértelműségi állítása.

3.1.19. Gyakorlat. Igazoljuk, hogy ha R alaptételes gyűrű, akkor tetszőleges $r, s \in R$ esetén $(r, s)[r, s]$ és rs asszociáltak.

3.1.20. Gyakorlat. Legyen R az $a + bi$ alakú számok gyűrűje a szokásos összeadásra és szorzásra, ahol $a, b \in \mathbb{Z}$ (ezek a Gauss-egészek, lásd 2.2.15. (2) Gyakorlat). Határozzuk meg 2-nek, és $1 + 3i$-nek az összes kitüntetett közös osztóját R-ben.

3.1.21. Feladat. Mutassuk meg, hogy a páros számok gyűrűjében nincsen olyan elem, amely minden elemnek osztója (ebben a gyűrűben), és nincsen prímtulajdonságú elem sem. Mik lesznek az asszociált elempárok? Igazoljuk, hogy minden elem felírható irreducibilisek szorzataként, de ez a felbontás nem mindig egyértelmű. Általánosítsuk a kapott észrevételeket nullosztómentes, kommutatív, de nem egységelemes gyűrűre.

3.1.22. Gyakorlat. Mutassuk meg, hogy a $\mathbb{Z}[x]$ gyűrűben a 2 és x elemeknek az 1 kitüntetett közös osztója, de ez nem írható föl $2p(x) + xq(x)$ alakban, ahol $p, q \in \mathbb{Z}[x]$.

3.1.23. Feladat. Legyen R az $a + bi\sqrt{5}$ alakú számok részgyűrűje $\mathbb{C}$-ben, ahol $a, b \in \mathbb{Z}$.

(1) Mutassuk meg, hogy a 3 ebben a gyűrűben felbonthatatlan, de nem prím.
(2) Létezik-e R-ben a 3-nak és a $2 + i\sqrt{5}$-nek kitüntetett közös osztója?
(3) Igaz-e R-ben a kitüntetett közös osztó kiemelési tulajdonsága (3.1.16. Gyakorlat)?

3.1.24. Feladat. Tekintsük az $\mathbb{R}[x, y]$ polinomgyűrűnek azokat az elemeit, amelyekben minden nem konstans tag legalább harmadfokú, de nem szerepel x^2y^2-es tag. Mutassuk meg, hogy ezek egy R részgyűrűt alkotnak, amely szokásos gyűrű, de nincs bármely két elemének kitüntetett közös osztója.

3.1.25. Gyakorlat. Legyen R azoknak a valós együtthatós „polinomoknak" a halmaza, amelyekben az x határozatlan kitevői nemcsak nemnegatív egész számok, hanem tetszőleges nemnegatív valós számok lehetnek. Mutassuk meg, hogy R elemei között az összeadás és szorzás a szokásos polinomokhoz hasonlóan elvégezhető, és így R szokásos gyűrű lesz, amelyben azonban az x nem bontható fel felbonthatatlanok szorzatára.

3.2. A maradékos osztás

Az előző szakaszban láttuk, hogy egész számok között a számelmélet alaptételét végső soron a maradékos osztás létezésének köszönhetjük. Test fölötti polinomgyűrűben szintén elvégezhető a maradékos osztás, és ezért itt is igaz lesz az alaptétel.

3.2.1. Tétel. *Legyen R szokásos gyűrű. Ekkor $R[x]$-ben minden olyan $g \in R[x]$ polinommal lehet maradékosan osztani, amelynek főegyütthatója invertálható. Ez azt jelenti, hogy tetszőleges $f \in R[x]$ polinomhoz léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = gq + r$, és vagy $r = 0$, vagy r foka kisebb g fokánál. A q és r polinomok egyértelműen meghatározottak.*

A most felírt maradékos osztásban a q polinomot *hányadosnak,* az r polinomot pedig *maradéknak* nevezzük. Az $r = 0$ esetet azért kellett külön vennünk, mert a nullapolinomnak nincsen foka.

Bizonyítás. Mint majd konkrét példákon látni fogjuk, polinomok között az osztást ahhoz hasonlóan kell elvégezni, ahogyan egész számok között (kézzel) maradékosan osztunk, még a jelölés is hasonló lesz. A most következő bizonyítás is ezt az eljárást követi: f foka szerinti indukcióval bizonyítjuk q és r létezését. Az $f = 0$ esetet ekkor külön meg kell nézni, de az rendben van, hiszen a $0 = g \cdot 0 + 0$ megfelelő lesz. Ha f foka kisebb g fokánál, akkor az $f = g \cdot 0 + f$ előállítás lesz megfelelő, és így az indukció kezdőlépését is megtettük.

Tegyük most fel, hogy f egy n-edfokú polinom, és hogy az n-nél kisebb fokú polinomokra már igaz az állítás. Jelölje f főtagját ax^n és g főtagját bx^m (ahol tehát b invertálható eleme R-nek). Mivel az m-nél kisebb fokú f polinomokra már beláttuk az állítást, feltehetjük, hogy $n \geq m$. Legyen $f_0 = f - (a/b)x^{n-m}g$. Ez értelmes, hiszen b-vel lehet osztani. A kivonásnál f főtagja kiesik, és így f_0 foka kisebb, mint n (vagy f_0 a nullapolinom). Az indukciós feltevés miatt f_0 maradékosan eloszthető g-vel: $f_0 = gq_0 + r$, ahol $r = 0$, vagy r foka kisebb g fokánál. De innen

$$f = f_0 + (a/b)x^{n-m}g = g\big(q_0 + (a/b)x^{n-m}\big) + r\,,$$

tehát f is eloszthető maradékosan g-vel.

Az egyértelműség bizonyításához tegyük fel, hogy f-et kétféleképpen is elosztottuk maradékosan g-vel:

$$f = gq_1 + r_1 = gq_2 + r_2\,,$$

ahol mind r_1, mind r_2 vagy nulla, vagy g-nél kisebb fokú polinom. Átrendezéssel

$$g(q_1 - q_2) = r_2 - r_1\,.$$

A jobboldalon álló $r_2 - r_1$ polinom vagy nulla, vagy g-nél kisebb fokú. Ha $q_1 - q_2 \neq 0$, akkor viszont a baloldalon álló polinom foka legalább annyi, mint g foka, hiszen szorzásnál a fokok összeadódnak, ami ellentmondás. Ezért $q_1 - q_2 = 0$, de akkor nyilván $r_2 - r_1 = 0$, és így a két maradékos osztásban a hányados és a maradék is ugyanaz. □

A tételből látjuk, hogy speciálisan test fölött minden nem nulla polinommal lehet maradékosan osztani. A bizonyításban szereplő $(a/b)x^{n-m}$ tag f és g főtagjainak hányadosa, ez lesz a keresett q hányados főtagja. Az osztás elvégzésekor ezzel kell beszorozni g-t, az eredményt f-ből kivonni, és a kapott polinommal ismételni az eljárást. Akkor állunk meg, amikor f foka már g foka alá csökken. Példaként osszuk el a $2x^3+2x^2+3x+2$ polinomot x^2+1-gyel:

$$\begin{array}{r} 2x^3+\ 2x^2+3x+2\ :\ x^2+1=\boxed{2x+2} \\ \underline{-(2x^3+\ \ 0\ \ +2x)} \\ 2x^2+\ x\ +2 \\ \underline{-\,(2x^2+\ 0\ \ +2)} \\ \boxed{x} \end{array}$$

Láthatjuk, hogy a hányados $2x+2$, a maradék pedig x.

Az osztásnál kapott hányados és maradék együtthatói természetesen az R gyűrű elemei. Ennek az észrevételnek, és a tétel egyértelműségi állításának van egy fontos következménye. Képzeljük el, hogy f és g racionális együtthatós polinomok, és g osztója f-nek a $\mathbb{C}[x]$ gyűrűben, vagyis létezik egy olyan $q \in \mathbb{C}[x]$ polinom, melyre $gq = f$. Azt állítjuk, hogy q minden együtthatója racionális szám, és így g már $\mathbb{Q}[x]$-ben is osztója f-nek.

Ez következik abból, ahogy az osztást végezzük, hiszen az $f : g$ kiszámításakor csak a négy alapműveletre van szükség, és megkapjuk q együtthatóit. Elegánsabb azonban az állítást a következőképpen bizonyítani. Osszuk el maradékosan f-et g-vel $\mathbb{Q}[x]$-ben:

$$f = gq_1 + r_1\,,$$

ahol $q_1, r_1 \in \mathbb{Q}[x]$ (és $r_1 = 0$ vagy $\mathrm{gr}(r_1) < \mathrm{gr}(g)$). Vessük össze ezt az

$$f = gq + 0$$

összefüggéssel. Ez két maradékos osztás $\mathbb{C}[x]$-ben. Az egyértelműség miatt tehát $q = q_1$, vagyis q tényleg racionális együtthatós.

Ugyanez a gondolatmenet működik abban az esetben is, ha $\mathbb{Q}$ vagy $\mathbb{C}$ helyett a valós számok teste szerepel. Az alábbi állítást ezért általánosan mondjuk ki: a $\mathbb{C}$ szerepét T, a $\mathbb{Q}$ szerepét S fogja játszani.

3.2.2. Állítás. *Legyen T test, és S részteste T-nek. Ha $f, g \in S[x]$, és g osztója f-nek $T[x]$-ben, akkor osztója $S[x]$-ben is.*

A kitüntetett közös osztó meghatározására szolgáló euklideszi algoritmus a maradékos osztáson alapszik, ezért tetszőleges test fölötti polinomgyűrűben is elvégezhető. Ezt az eljárást röviden átismételjük. Legyen T test, és $f, g \in T[x]$ két polinom. Készítsük el az alábbi maradékos osztásokat:

$$\begin{aligned} f &= gq_1 &&+ r_1 \\ g &= r_1q_2 &&+ r_2 \\ r_1 &= r_2q_3 &&+ r_3 \\ &\dots \\ r_{n-2} &= r_{n-1}q_n &&+ r_n \\ r_{n-1} &= r_nq_{n+1} &&+ 0\,. \end{aligned}$$

Az itt szereplő $r_1, r_2, \dots$ maradékok foka egyre csökken, és mivel ezek a fokok nemnegatív egész számok, előbb-utóbb a maradék nulla lesz. A jelölést úgy választottuk, hogy r_n

legyen az utolsó nem nulla maradék. Az egész számokra tanult bizonyítás szó szerint átvihető: r_n az f és g kitüntetett közös osztója lesz.

3.2.1. Gyakorlat. Mutassuk meg, hogy a fenti eljárásban kapott legutolsó nem nulla maradék, vagyis az r_n polinom az f és g polinomok kitüntetett közös osztója, és ez előállítható $fp + gq$ alakban, ahol p és q alkalmas $T[x]$-beli polinomok.

3.2.2. Feladat. Az euklideszi algoritmus fenti vázlatában több pontatlanság is van. Keressük meg, és javítsuk ki ezeket.

Mint tudjuk, a kitüntetett közös osztó csak asszociáltság erejéig egyértelmű. Azt is láttuk (a 3.1.7. Gyakorlatban), hogy egy test fölött két polinom akkor és csak akkor asszociált, ha egymás konstansszorosai. Néha meg szokás állapodni abban, hogy az (f, g) jelölés a kitüntetett közös osztók közül az egyetlen normált polinomot jelöli.

3.2.3. Gyakorlat. Mutassuk meg, hogy két racionális együtthatós polinom $\mathbb{Q}[x]$-beli kitüntetett közös osztója $\mathbb{C}[x]$-ben is kitüntetett közös osztó. Általánosítsuk az állítást.

Most még egy bizonyítást adunk arra, hogy test fölötti polinomgyűrűben létezik a kitüntetett közös osztó. Ez a bizonyítás egyszerűbb, mint a fenti, és bevezeti azt a módszert, amellyel később a számelméleti kérdéseket gyűrűkben vizsgálni fogjuk. Hátránya, hogy segítségével nem lehet kiszámítani a kitüntetett közös osztót, erre a célra továbbra is az euklideszi algoritmust használjuk majd.

3.2.3. Tétel. *Legyen T test. Ekkor tetszőleges két T fölötti f és g polinomnak létezik az (f, g) kitüntetett közös osztója. Ha h is egy T fölötti polinom, akkor h pontosan akkor írható föl $fp + gq$ alakban alkalmas $p, q \in T[x]$ polinomokkal, ha $(f, g) \mid h$.*

Bizonyítás. Jelölje I az $fp + gq$ alakban felírható polinomok halmazát, ahol $p, q \in T[x]$. Ennek a halmaznak több érdekes tulajdonsága is van. Például zárt az összeadásra. Valóban, ha $h_1, h_2 \in I$, akkor

$$h_1 = fp_1 + gq_1 \quad \text{és} \quad h_2 = fp_2 + gq_2$$

alkalmas $p_1, p_2, q_1, q_2 \in T[x]$ polinomokra. De akkor

$$h_1 + h_2 = f(p_1 + p_2) + g(q_1 + q_2)\,,$$

ami azt mutatja, hogy $h_1 + h_2 \in I$.

Az I másik fontos tulajdonsága, hogy minden elemének az összes többszörösét (polinomszorosát) is tartalmazza (ez tehát több, mintha csak azt mondanánk, hogy részgyűrű). Valóban, ha $h \in I$, azaz $h = fp + gq$, és $r \in T[x]$ egy tetszőleges polinom, akkor

$$hr = f(pr) + g(qr) \in I\,.$$

Válasszunk ki most I-ből egy olyan h_0 polinomot, aminek a foka a lehető legkisebb. Megmutatjuk, hogy az I elemei pont a h_0 többszörösei. Azt az előbb láttuk, hogy h_0

többszörösei benne vannak I-ben. Megfordítva, ha $h \in I$ tetszőleges, akkor osszuk el h-t maradékosan h_0-lal:

$$h = h_0 q + r\,,$$

ahol $r = 0$, vagy r foka kisebb, mint h_0 foka. Az első esetben készen is vagyunk, hiszen azt akarjuk belátni, hogy h többszöröse h_0-nak. Ha $r \neq 0$, akkor

$$r = h - h_0 q \in I\,,$$

hiszen I-ben benne van $-h_0 g$ is (hiszen ez h_0 többszöröse), és benne van h is, tehát benne van a kettő összege is. De ez lehetetlen, mert r foka kisebb, mint h_0 foka, és h_0 foka a lehető legkisebb volt az I-beli elemek fokai között. Tehát beláttuk, hogy I tényleg a h_0 többszöröseiből áll.

Most azt mutatjuk meg, hogy h_0 kitüntetett közös osztója f-nek és g-nek. Nyilván $f \in I$ (mert $f = f \cdot 1 + g \cdot 0$), és hasonlóképpen $g \in I$. Így h_0 osztója f-nek és g-nek. Tegyük most fel, hogy $k \in T[x]$ közös osztója f-nek és g-nek, be kell látni, hogy $k \mid h_0$. De ez nyilvánvaló, hiszen $h_0 \in I$, azaz h_0 felírható $fp + gq$ alakban. Tehát h_0 tényleg f és g kitüntetett közös osztója.

Végül vegyük észre, hogy menet közben beláttuk a tétel utolsó állítását is. Az I halmaz ugyanis azokból a h polinomokból áll, amik felírhatók $fp + gq$ alakban, és éppen azt mutattuk meg, hogy ezek a polinomok $h_0 = (f, g)$ többszörösei. □

3.2.4. Feladat. Az előző bizonyításban van egy apró pontatlanság. Keressük ezt meg, és tegyük teljessé a gondolatmenetet.

Az eddig elmondottakból már könnyen következik az, hogy minden test fölötti polinomgyűrű alaptételes, vagyis minden polinom egyértelműen bontható irreducibilisek szorzatára. Először tisztázzuk, hogy test fölött mit is jelent az irreducibilitás.

3.2.4. Állítás. *Legyen T test. Egy $f \in T[x]$ polinom akkor és csak akkor irreducibilis T fölött, ha nem konstans, és nem bontható fel két alacsonyabb fokú T-beli együtthatós polinom szorzatára.*

Bizonyítás. Test fölött az egységek a nem nulla konstans polinomok (3.1.7. Gyakorlat). Tehát egy polinom triviális felbontásai azok, amikor az egyik tényező konstans, és így a nemtriviális felbontások azok, amikor egyik tényező sem konstans. Ez ugyanazt jelenti, mintha azt mondanánk, hogy mindkét tényező az eredeti polinomnál alacsonyabb fokú kell, hogy legyen, hiszen a tényezők fokainak összege az eredeti polinom foka. □

Vigyázzunk, a most adott jellemzés általános gyűrű fölött már nem működik. Ezzel a jelenséggel a 3.4. Szakaszban fogunk érdemben foglalkozni, most csak egy gyakorlat erejéig mutatjuk be.

3.2.5. Gyakorlat. Irreducibilis-e a $2x$ polinom $\mathbb{Z}$ fölött?

3.2.5. Tétel. *Legyen T test. Ekkor $T[x]$-ben érvényes a számelmélet alaptétele.*

Ennek a tételnek a bizonyítását most csak két feladat formájában, vázlatosan ismertetjük. Ennek egyrészt az az oka, hogy a gondolatmenet lényegében ugyanaz, mint az egész számok esetében, másrészt pedig az, hogy később a gyűrűelméleti részben egy olyan általános eredményt bizonyítunk majd, amelynek ez a tétel speciális esete lesz.

3.2.6. Feladat. Mutassuk meg, hogy ha T test, akkor $T[x]$-ben minden irreducibilis polinom prímtulajdonságú. Vezessük le ebből a számelmélet alaptételének egyértelműségi állítását.

3.2.7. Feladat. Mutassuk meg, hogy ha T test, akkor minden nem konstans $T[x]$-beli polinom felbontható irreducibilis polinomok szorzatára.

Az euklideszi algoritmusnak másik fontos alkalmazása, hogy lehetővé teszi két polinom közös gyökeinek megkeresését. Természetesen ez akkor izgalmas, ha a gyököket különkülön nem tudjuk meghatározni.

3.2.6. Állítás. *Legyen R szokásos gyűrű és $f, g \in R[x]$. Ha létezik az (f, g) kitüntetett közös osztó, akkor ennek az R-beli gyökei pontosan az f és g közös gyökei.*

Bizonyítás. Ha $b \in R$ gyöke (f, g)-nek, akkor gyöke mindegyik többszörösének is, azaz f-nek is és g-nek is. Ha viszont $b \in R$ közös gyöke f-nek és g-nek, akkor $x - b$ osztója mindkét polinomnak, és így a kitüntetett közös osztójuknak is. □

Gyakorlatok, feladatok

3.2.8. Gyakorlat. Osszuk el maradékosan az $x^3 - 2$ polinomot $2x^2 + 2x - 3$-mal.

3.2.9. Gyakorlat. Az alábbi f és g polinomoknak határozzuk meg a kitüntetett közös osztóját az euklideszi algoritmussal, és az eredményt a visszahelyettesítési eljárással írjuk fel $fp + gq$ alakban, ahol p és q alkalmas polinomok.

(1) $f(x) = 3x^3 + 6x^2 + 6x + 3$ és $g(x) = 2x^4 + 2x^2 + 2$.
(2) $f(x) = x^5 - 1$ és $g(x) = x^3 - 1$.

3.2.10. Gyakorlat. Elvégezhető-e $\mathbb{Z}[x]$-ben az $x : 2$ maradékos osztás? Vagyis léteznek-e olyan $q, r \in Z[x]$ polinomok, hogy $x = 2q(x) + r(x)$, és $r = 0$, vagy r foka kisebb a 2 fokánál?

3.2.11. Gyakorlat. Tegyük fel, hogy f és $g \neq 0$ egész együtthatós polinomok. Igaz-e, hogy g akkor és csak akkor osztója f-nek $\mathbb{Z}[x]$-ben, ha az $f : g$ maradékos osztást $\mathbb{Q}[x]$-ben elvégezve a hányados egész együtthatós, és a maradék nulla?

3.2.12. Gyakorlat. Legyen T test, és S részgyűrűje T-nek. Tegyük fel, hogy $f, g \in S[x]$, és g főegyütthatója invertálható S-ben. Mutassuk meg, hogy ha g osztója f-nek $T[x]$-ben, akkor osztója $S[x]$-ben is.

3.2.13. Gyakorlat. Vezessük le a gyöktényező kiemelhetőségéről szóló 2.4.4. Állítást a maradékos osztás tételéből.

3.2.14. Gyakorlat. Mi lesz a maradék, ha az $x^4 + x^2 + 1$ polinomot elosztjuk $x^2 + x + 1$-gyel? A kapott eredményt indokoljuk meg számolás nélkül is. Hogyan lehetne általánosítani a kapott észrevételt?

3.2.15. Gyakorlat. Mi a maradék, ha $x^{64} + x^{54} + x^{14} + 1$-et osztjuk $x^2 - 1$-gyel, illetve $x^2 + 1$-gyel?

3.2.16. Gyakorlat. Ha b közös gyöke az f és g (szokásos gyűrű fölötti) polinomoknak, és h kitüntetett közös osztója f-nek és g-nek, akkor mi lesz a b gyök multiplicitása h-ban?

3.2.17. Feladat. Határozzuk meg az egész számok gyűrűjében az összes olyan nem üres I részhalmazt, amely zárt az összeadásra, és bármely elemének mindegyik többszörösét is tartalmazza. Hogyan használhatnánk fel a kapott eredményt a komplex szám rendjére vonatkozó 1.5.4. Tétel egyszerűbb bizonyítására?

3.3. Gyökök és irreducibilitás

Általában nehéz feladat egy polinomról eldönteni, hogy irreducibilis-e. A későbbiekben (az úgynevezett Galois-elmélet keretében) új eszközöket találunk majd az irreducibilitás vizsgálatára. Most először azt tekintjük át, hogy egy test fölötti polinom irreducibilitása hogyan függ össze azzal: van-e gyöke az adott testben. Emlékeztetjük az olvasót a 3.2.4. Állításra, mely szerint egy *test fölötti* polinom akkor és csak akkor irreducibilis, ha nem konstans, és *nem bontható fel két alacsonyabb fokú polinom szorzatára.*

3.3.1. Állítás. *Test fölött egy elsőfokú polinom mindig irreducibilis.*

Bizonyítás. Elsőfokú polinomot nem lehet alacsonyabb fokúak szorzatára bontani, hiszen két nulladfokú polinom szorzata is nulladfokú. □

3.3.2. Állítás. *Legyen T test.* ***Ha*** *egy legalább másodfokú $T[x]$-beli polinomnak* ***van gyöke*** *T-ben,* ***akkor nem irreducibilis*** *T fölött.*

Bizonyítás. Legyen $b \in T$ gyöke egy $f \in T[x]$ polinomnak. Ekkor a hozzá tartozó $x - b$ gyöktényező kiemelhető f-ből. Ha f legalább másodfokú, akkor ezzel f-et két alacsonyabb fokú polinom szorzatára bontottuk. □

Ennek az észrevételnek a kapcsán az embernek az az érzése támadhat, hogy az irreducibilitás eldöntéséhez elég a gyököket megkeresni. De ez nem így van! ***Abból, hogy egy polinomnak nincs gyöke, még nem következik, hogy irreducibilis!*** A legegyszerűbb példa az $(x^2 + 1)^2$ polinom a racionális test fölött. Ennek még valós gyöke sincs, és nyilván nem irreducibilis, hiszen eleve szorzatként adtuk meg. A gyökök ismerete tehát nem csodafegyver az irreducibilitás eldöntéséhez, de hasznos, mert ha véletlenül találunk gyököt, akkor már készen is vagyunk.

3.3.3. Állítás. *Legyen T test. Ekkor egy $f \in T[x]$ polinomnak akkor és csak akkor van gyöke T-ben, ha van* ***elsőfokú*** *tényezője.*

Bizonyítás. Azt már láttuk, hogy ha van gyök, akkor a megfelelő gyöktényező kiemelhető. Megfordítva, tegyük fel, hogy $f = gh$, ahol $g(x) = ax + b$ egy elsőfokú polinom. Ekkor $-b/a$ gyöke f-nek. □

A gyök létezése tehát elsőfokú tényezőt jelent. Egy reducibilis polinom azonban bomolhat csupa egynél magasabb fokú tényezőre is, és *ezért* nem biztos, hogy van gyöke. Van azonban egy speciális helyzet, amikor elegendő a polinom gyökeit ellenőrizni az irreducibilitás eldöntéséhez.

3.3.4. Állítás. *Legyen T test. Ha egy* ***másod- vagy harmadfokú*** *$T[x]$-beli polinomnak nincs gyöke T-ben, akkor irreducibilis T fölött.*

Bizonyítás. Egy másodfokú polinomot alacsonyabb fokú tényezők szorzatára csak úgy lehet felbontani, hogy mindkét tényező elsőfokú lesz. Hasonlóképpen egy harmadfokú polinomot alacsonyabb fokúak szorzatára csak úgy bonthatunk, hogy az egyik tényező elsőfokú, a másik pedig másodfokú lesz. Mindkét esetben lesz tehát elsőfokú tényező, és így az előző állítás szerint gyök is. □

Most, hogy az irreducibilitás és a gyökök viszonyát tisztáztuk, megpróbáljuk tudásunkat alkalmazni néhány konkrét test esetében.

3.3.5. Tétel. *A komplex számok teste fölött (és általában egy algebrailag zárt T test fölött) az irreducibilis polinomok pontosan az elsőfokúak.*

Bizonyítás. Ez nyilvánvaló az eddigiekből, hiszen algebrailag zárt test fölött minden nem konstans polinomnak van gyöke. □

A valós számok teste fölötti irreducibilitás vizsgálatához egy nagyon hasznos segédállításra van szükségünk.

3.3.6. Lemma. *Legyen f valós együtthatós polinom, és z egy komplex gyöke f-nek. Ekkor z konjugáltja is gyöke f-nek, sőt z és $\overline{z}$ ugyanannyiszoros gyökök.*

Bizonyítás. Legyen $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Ennek gyöke a z, tehát

$$a_0 + a_1z + \cdots + a_nz^n = 0\,.$$

Vegyük mindkét oldal konjugáltját. Tudjuk, hogy összeg konjugáltja a konjugáltak összege, és ezért a baloldalon álló összeget tagonként konjugálhatjuk. De a konjugálás szorzattartó is, ezért az eredmény ez lesz:

$$\overline{a_0} + \overline{a_1}\,\overline{z} + \cdots + \overline{a_n}\,\overline{z}^n = \overline{0}\,.$$

Valós szám konjugáltja önmaga, tehát $\overline{0} = 0$ és $\overline{a_j} = a_j$. Így a baloldalon $f(\overline{z})$ áll, a jobboldalon 0, tehát $\overline{z}$ tényleg gyöke f-nek.

A lemma második állítását f foka szerinti indukcióval bizonyítjuk. Ha z valós, azaz $z = \overline{z}$, akkor az állítás nyilvánvaló. Ha nem, azaz ha $z \neq \overline{z}$, akkor a z és $\overline{z}$ gyökökhöz tartozó gyöktényezők (a 2.4.5. Tétel miatt) egyszerre is kiemelhetők:

$$f(x) = (x - z)(x - \overline{z})q(x)$$

alkalmas $q \in \mathbb{C}[x]$ polinomra. Azonban

$$g(x) = (x - z)(x - \overline{z}) = x^2 - (z + \overline{z}) + z\overline{z}$$

valós együtthatós polinom, hiszen $z\overline{z} = |z|^2$ és $z+\overline{z} = 2\operatorname{Re} z$ valós számok. A 3.2.2. Állítás (igazából a maradékos osztás egyértelműsége) miatt q is valós együtthatós polinom. Az indukciós feltevés miatt tehát q-nak z és $\overline{z}$ ugyanannyiszoros (esetleg nullaszoros) gyöke, és így ugyanez igaz f-re is. □

3.3.7. Tétel. *A valós számok teste fölött az irreducibilis polinomok pontosan az elsőfokúak, és azok a másodfokúak, melyeknek nincs valós gyöke.*

Bizonyítás. A felsorolt polinomokról a korábbi állításokban már beláttuk, hogy irreducibilisek. Tegyük fel, hogy f irreducibilis polinom $\mathbb{R}$ fölött. Ekkor nem konstans, és így van egy z komplex gyöke. Ha ez valós, akkor f csak elsőfokú lehet. Ha z nem valós, akkor az előző bizonyításban láttuk, hogy a valós együtthatós $g(x) = (x - z)(x - \overline{z})$ kiemelhető f-ből, és a megmaradó q polinom is valós együtthatós. Mivel f irreducibilis, $q(x)$ csak konstans lehet, és így f tényleg másodfokú, melynek gyökei nem valósak. □

3.3.8. Következmény. *Páratlan fokú valós együtthatós polinomnak van valós gyöke.*

Erre az állításra két bizonyítást is adunk. Az első bizonyítás itt szerepel, ebben felhasználjuk az algebra alaptételét. A második bizonyítás az A. Függelékben található (lásd A.0.4. Tétel), az csak elemi analízist használ, az algebra alaptételét nem.

Már említettük, hogy az algebra alaptételének bizonyításához valamennyi analízis-tudás is szükséges, és ha komplex függvénytant is használhatunk, akkor nagyon egyszerű lesz a bizonyítás. Van azonban egy nagyon elegáns bizonyítás Galois-elmélet felhasználásával is, ezt a 6.3. Szakaszban fogjuk bemutatni. Az abban felhasznált analízis-ismeretek minimálisak: semmi másra nincs szükség, mint a most bizonyítandó 3.3.8. Állításra. Ezért adunk erre az állításra az algebra alaptételétől független bizonyítást is.

Bizonyítás. Bontsuk a polinomot irreducibilisek szorzatára $\mathbb{R}$ fölött. Ezek első- vagy másodfokúak. Mindegyik tényező nem lehet másodfokú, mert a polinom foka páratlan. Tehát van elsőfokú tényező, és így valós gyök is. □

A racionális számok teste fölött már nem tudjuk olyan könnyen leírni az irreducibilis polinomokat, mint $\mathbb{C}$ és $\mathbb{R}$ fölött. Itt vannak akárhányadfokú irreducibilis polinomok is: nemsokára látni fogjuk, hogy például $x^n - 2$ irreducibilis $\mathbb{Q}$ fölött tetszőleges $n \geq 1$ esetén. A most bizonyított eredmények mégis segíthetnek néha, mert ha találunk egy racionális gyököt, akkor tudjuk, hogy a polinom nem lehet irreducibilis (kivéve ha elsőfokú). Az alábbiakban egy eljárást ismertetünk a racionális gyökök megkeresésére.

Ha adott egy racionális együtthatós polinom, akkor szorozzuk be az együtthatók nevezőivel. Így egy egész együtthatós polinomot kapunk, amelynek a gyökei ugyanazok, mint a kiinduló polinomé. Így elegendő az egész együtthatós polinomok racionális gyökeit megkeresni. Erre szolgál az alábbi állítás.

3.3.9. Tétel [Racionális gyökteszt]. *Tegyük fel, hogy a p/q már nem egyszerűsíthető tört gyöke az f egész együtthatós polinomnak. Ekkor a számláló (azaz p) osztja f konstans tagját, a nevező (azaz q) pedig osztja f főegyütthatóját.*

Azt nem állítjuk, hogy a feltételnek eleget tevő törtek tényleg gyökei az f polinomnak! De csak véges sok törtről van szó, mert a főegyütthatónak és a konstans tagnak is (ha nem nulla) véges sok osztója van. Így ezeket a törteket egyenként végigpróbálgathatjuk: mindegyiket behelyettesíthetjük (például a Horner-elrendezéssel) az f polinomba. Ezzel megkapjuk az f összes racionális gyökét.

Bizonyítás. Az, hogy a tört már nem egyszerűsíthető, azt jelenti, hogy p és q relatív prím egész számok. Legyen $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Ekkor p/q-t behelyettesítve, majd q^n-nel beszorozva

$$a_0q^n + a_1pq^{n-1} + \cdots + a_np^n = 0$$

adódik. Ebben az összegben mindegyik tag osztható p-vel, kivéve esetleg a legelsőt. Mivel a 0 is osztható p-vel, ezért a legelső tag is, tehát $p \mid a_0q^n$. De p és q relatív prímek, és így $p \mid a_0$. Ugyanezzel a módszerrel kapjuk a $q \mid a_n$ oszthatóságot is. □

3.3.1. Gyakorlat. Hogyan alkalmazhatjuk a racionális gyöktesztet egy olyan polinom racionális gyökeinek a megkeresésére, amelynek a konstans tagja nulla?

A $\mathbb{Q}$ fölötti irreducibilitás eldöntésében néha segíthet az, ha a polinomnak a komplex gyökeit ismerjük. Ennek a módszernek az illusztrálására egy példát dolgozunk ki.

3.3.10. Példa. Mutassuk meg, hogy $x^4 + 36$ irreducibilis $\mathbb{Q}$ fölött.

Határozzuk meg a polinom komplex gyökeit. A -36 számból (például trigonometrikus alak segítségével) negyedik gyököt vonva az eredmény $\sqrt{3}(\pm 1 \pm i)$. A gyöktényezős alak tehát a következő:

$$x^4 + 36 = \big(x - \sqrt{3} - \sqrt{3}i\big)\big(x - \sqrt{3} + \sqrt{3}i\big)\big(x + \sqrt{3} - \sqrt{3}i\big)\big(x + \sqrt{3} + \sqrt{3}i\big)\,.$$

Egyik gyök sem valós, és így ha $x^4 + 36$ felbomlik $\mathbb{Q}$ fölött, akkor csak két másodfokú polinom szorzata lehet: $x^4 + 36 = f(x)g(x)$. Az f és g gyökei összesen kiadják a fenti négy komplex gyököt. Mivel f és g valós együtthatósak, gyökeik konjugáltak kell, hogy legyenek. Ezért f és g egyike

$$r\big(x - \sqrt{3} - \sqrt{3}i\big)\big(x - \sqrt{3} + \sqrt{3}i\big) = r\big(x^2 - 2\sqrt{3}x + 6\big)\,,$$

a másik pedig

$$s\big(x + \sqrt{3} - \sqrt{3}i\big)\big(x + \sqrt{3} + \sqrt{3}i\big) = s\big(x^2 + 2\sqrt{3}x + 6\big)\,,$$

alkalmas r és s (nem nulla) valós számokra (a beszorzást, a 2.5.5. Gyakorlat megoldásához hasonlóan, az $(a-b)(a+b) = a^2 - b^2$ azonosság felhasználásával érdemes elvégezni). Mivel f és g racionális együtthatós, a fenti első polinom főegyütthatója, azaz r is racionális szám. Racionális továbbá ebben a polinomban x együtthatója, azaz $-2r\sqrt{3}$ is, ami lehetetlen, hiszen akkor $\sqrt{3}$ is racionális lenne. Ezért $x^4 + 36$ tényleg irreducibilis $\mathbb{Q}$ fölött.

Gyakorlatok, feladatok

3.3.2. Gyakorlat. Bontsuk fel a következő polinomokat az $\mathbb{R}$ fölött irreducibilis polinomok szorzatára: $x^4 - 1,\ x^4 + 1,\ x^4 + 9,\ x^6 - 4x^3 + 3$.

3.3.3. Gyakorlat. Bontsuk fel a $6(x^2 - 2)(x^2 + 1)$ polinomot $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ fölött felbonthatatlanok szorzatára.

3.3.4. Gyakorlat. Adjuk meg az összes olyan tizenkettedfokú valós együtthatós polinomot, melynek az $1 + i$ hatszoros gyöke.

3.3.5. Gyakorlat. Adjuk meg a $2x^3 + 3x + 5$ polinom racionális gyökeit, és bontsuk $\mathbb{Q}$ fölött irreducibilisek szorzatára.

3.3.6. Gyakorlat. Legyen c pozitív egész szám. Mi annak a szükséges és elégséges feltétele, hogy $x^4 + c$ irreducibilis legyen $\mathbb{R}$, illetve $\mathbb{Q}$ fölött? Mi a helyzet negatív c esetén?

3.3.7. Gyakorlat. Határozzuk meg a $\mathbb{Z}_2$ test fölött a legfeljebb negyedfokú irreducibilis polinomokat.

3.3.8. Feladat. Legyen $p \in \mathbb{Z}$ pozitív prímszám, és R olyan gyűrű, amelyben minden elem p-szerese nulla. Bizonyítsuk be, hogy tetszőleges $r, s \in R$ elemekre

$$(r + s)^p = r^p + s^p\,,$$

azaz R-ben tagonként lehet p-edik hatványra emelni. Vezessük le ebből a kis Fermat Tételt (miszerint $b^p - b$ osztható p-vel minden b egészre). Mutassuk meg, hogy tetszőleges $f \in \mathbb{Z}_p[x]$ polinomra $f(x^p) = f(x)^p$.

3.3.9. Gyakorlat. Irreducibilisek-e az alábbi polinomok?

(1) $\mathbb{Z}_2$ fölött $x^8 + x^2 + 1,\ x^5 + x + 1,\ \ x^5 + x^3 + 1,\ x^5 + x^4 + x^3 + 1$.
(2) $\mathbb{Z}_{17}$ fölött $x^2 + 1,\ x^4 + 1,\ x^8 + 1,\ x^{17} + 1,\ x^{17} + 2$.

3.3.10. Feladat. Bontsuk fel az $x^4 - 10x^2 + 1$ polinomot $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ fölött felbonthatatlanok szorzatára.

3.4. Egész együtthatós polinomok

Ebben a szakaszban a $\mathbb{Z}[x]$ számelméletét vizsgáljuk. Erről a gyűrűről is be fogjuk látni, hogy igaz benne az alaptétel, de másképp, mint test fölötti polinomokra, mert $\mathbb{Z}[x]$-ben nem végezhető el korlátlanul a maradékos osztás. A kapott eredmények segíteni fognak a $\mathbb{Q}$ fölötti irreducibilitás vizsgálatában is.

A $\mathbb{Q}$ és $\mathbb{Z}$ számelmélete közötti első különbséggel már szembesült az, aki megoldotta a 3.2.5. Gyakorlatot. A $2x$ polinom $\mathbb{Q}$ fölött irreducibilis, de $\mathbb{Z}$ fölött nem az, mert itt a $2 \cdot x$ felbontás nem triviális: a 2 egység $\mathbb{Q}$ fölött, de nem egység $\mathbb{Z}$ fölött.

Ha tehát egy egész együtthatós polinomot $\mathbb{Z}$ fölött akarunk felbontani, akkor úgy érdemes kezdeni, hogy kiemeljük belőle azt az egész számot, amit lehet, vagyis az együtthatóinak a legnagyobb közös osztóját. Például

$$180x^3 + 72x + 120 = 12(15x^3 + 6x + 10)\,.$$

A megmaradó polinomot primitívnek fogjuk nevezni. Tehát $15x^3 + 6x + 10$ már primitív polinom.

3.4.1. Definíció. Egy egész együtthatós nem nulla polinomot *primitívnek* nevezünk, ha együtthatóinak legnagyobb közös osztója 1.

E definíció egytagú polinom esetében azt jelenti, hogy az egyetlen nem nulla együttható ± 1 (ez felel meg annak a szemléletnek, hogy a polinomból csak egységet lehessen kiemelni). De ezt nem szükséges külön kikötni, mert együtthatók legnagyobb közös osztóján az $(a, 0) = a$ összefüggés miatt nem változtat, ha nulla együtthatókat is közéjük veszünk.

A polinomból kiemelt egész számot úgy bontjuk fel, mint az egész számok között. Ez azért lesz megfelelő, mert az egészek közötti felbonthatatlan számok a polinomok között is felbonthatatlanok.

3.4.1. Gyakorlat. Mutassuk meg, hogy a felbonthatatlan egész számokat konstans polinomnak képzelve $\mathbb{Z}[x]$-ben is felbonthatatlan elemeket kapunk.

A számelmélet alaptétele kapcsán láttuk, hogy a felbonthatatlan egész számok prímtulajdonságúak. A $\mathbb{Z}[x]$-beli alaptétel bizonyításának első lépése az, hogy belátjuk: ezek a számok prímtulajdonságúak $\mathbb{Z}[x]$-ben is.

3.4.2. Lemma [Első Gauss Lemma]. *Ha p prímszám, akkor $\mathbb{Z}[x]$-ben mint konstans polinom is prímtulajdonságú.*

Bizonyítás. A lemmára két bizonyítást is adunk. Az első elemi számolás lesz. A második elegánsabb, felhasználja a modulo p számolásról tanultakat. Azt tudjuk, hogy p nem nulla, és nem ± 1, tehát $\mathbb{Z}[x]$-ben sem egység. Tegyük fel, hogy $p \mid fg$, ahol $f, g \in \mathbb{Z}[x]$. Meg kell mutatni, hogy $p \mid f$ vagy $p \mid g$.

Az első bizonyításban felírjuk f és g együtthatóit, és elvégezzük a szorzást. Legyen

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \quad \text{és} \quad g(x) = b_0 + b_1x + \cdots + b_mx^m\,.$$

Tegyük fel, hogy p nem osztója sem f-nek, sem g-nek, azaz mindkét polinomnak van p-vel nem osztható együtthatója. Válasszuk ki mindkét polinomban a legnagyobb indexű ilyen együtthatót, legyenek ezek a_i és b_j. Tudjuk, hogy fg-ben az x^{i+j} együtthatója

$$a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0$$

(ahol a szokásos konvenció szerint $a_{n+1} = a_{n+2} = \cdots = 0$ és $b_{m+1} = b_{m+2} = \cdots = 0$). Az összeg tagjai egy kivétellel mind p-vel oszthatók, mert az a_i választása (az i maximalitása) miatt $a_{i+1}, \ldots, a_{i+j}$, a b_j választása miatt pedig $b_{j+1}, \ldots, b_{i+j}$ osztható p-vel.

A kimaradó $a_i b_j$ viszont nem osztható p-vel, mert a_i és b_j nem osztható p-vel, és p prímszám. Tehát a fenti összeg nem osztható p-vel. Ez lehetetlen, mert ez az összeg a p-vel osztható fg polinom egyik együtthatója. Ez az ellentmondás bizonyítja az állítást.

A második bizonyítást az elsőből származtathatjuk, ha észrevesszük, hogy az elmondott gondolatmenet mennyire hasonlít annak bizonyításához, hogy szorzatpolinom foka a fokok összege. Ezt a hasonlóságot ki is aknázhatjuk, ha az f és g polinomokat (pontosabban az együtthatóikat) modulo p vesszük. Ekkor ugyanis az iménti gondolatmenetben kiválasztott a_i az f polinom főegyütthatójává, a b_j pedig a g polinom főegyütthatójává válik.

A második bizonyítás tehát a következőképpen hangzik. Vegyük az f, g és fg polinomokat modulo p, az eredményt jelölje $\overline{f}$, $\overline{g}$, $\overline{fg} \in \mathbb{Z}_p[x]$. Ekkor $\overline{fg} = \overline{f}\ \overline{g}$ (a 2.3.4. Gyakorlat miatt). Mivel $p \mid fg$, az $\overline{fg}$ a nullapolinom. De $\mathbb{Z}_p$ test, és így $\mathbb{Z}_p[x]$ nullosztómentes. Tehát $\overline{f}$ és $\overline{g}$ egyike nulla, vagyis f és g egyike osztható p-vel. □

Néha az előző állítás alábbi következményét is „első Gauss-lemma" néven emlegetik.

3.4.3. Következmény [Első Gauss Lemma, első következmény]. *Primitív polinomok szorzata is primitív.*

Bizonyítás. Tegyük fel, hogy $f, g \in \mathbb{Z}[x]$ primitív polinomok. Azt kell megmutatni, hogy fg nem osztható egységtől különböző egész számmal. Ha osztható lenne, akkor lenne egy p prímosztója is. Az előző lemma miatt ekkor $p \mid f$ vagy $p \mid g$, ami nem lehet, hiszen f és g primitívek. □

3.4.4. Következmény [Első Gauss Lemma, második következmény]. *Legyen f primitív (egész együtthatós) polinom. Ha g olyan racionális együtthatós polinom, melyre $h = fg$ egész együtthatós, akkor g is egész együtthatós. Speciálisan ha f osztója egy h egész együtthatós polinomnak $\mathbb{Q}[x]$-ben, akkor f osztója h-nak $\mathbb{Z}[x]$-ben is.*

Bizonyítás. Hozzuk g együtthatóit közös nevezőre, és emeljük ki a számlálókból a legnagyobb közös osztójukat. Így a $g = (s/t)g_0$ felbontást kapjuk, ahol g_0 már primitív (egész együtthatós) polinom, és az s, t egész számokról az s/t törtet egyszerűsítve feltehetjük, hogy relatív prímek. A $h = fg$ egyenlőséget t-vel megszorozva kapjuk, hogy $th = sfg_0$. Ha p prímosztója t-nek, akkor $p \mid sfg_0$, az első Gauss-lemma miatt tehát $p \mid s$, vagy $p \mid f$, vagy $p \mid g_0$. Mindhárom lehetetlen, az első azért, mert t és s relatív prímek, a másik kettő azért, mert f és g_0 primitívek. A t számnak nincs tehát prímosztója, vagyis t egység, és így $g = (s/t)g_0$ tényleg egész együtthatós polinom. □

Az előző bizonyításban láttuk, hogy minden racionális együtthatós polinom felbontható egy racionális szám, és egy egész együtthatós primitív polinom szorzatára. Az alábbi gyakorlat ennek a felbontásnak az egyértelműségét fogalmazza meg.

3.4.2. Gyakorlat. Mutassuk meg, hogy minden nem nulla racionális együtthatós polinom felírható egy egész együtthatós primitív polinom és egy racionális szám szorzataként, és a felbontásban szereplő primitív polinom $\mathbb{Z}$ fölötti asszociáltság erejéig egyértelműen meghatározott.

A $\mathbb{Z}[x]$-beli alaptételt a $\mathbb{Q}[x]$-beli alaptétel segítségével fogjuk bizonyítani. Ehhez meg kell vizsgálnunk, hogy egy adott polinomnak „mennyivel több" felbontása van $\mathbb{Q}$, mint $\mathbb{Z}$ fölött. Ha a polinom $f(x) = x^2 - 1$, akkor ennek $\mathbb{Q}$ fölött felbontása lesz például a következő:

$$x^2 - 1 = \big((2/3)x - (2/3)\big)\big((3/2)x + (3/2)\big).$$

Mindannyian érezzük, hogy ez „valójában" az $(x-1)(x+1)$ felbontás, csak „el van bonyolítva" úgy, hogy az első tényezőt $2/3$-dal, a másodikat $3/2$-del beszoroztuk. Gauss második lemmája azt mondja ki, hogy minden $\mathbb{Q}$ fölötti felbontás egy $\mathbb{Z}$ fölötti felbontás hasonló „elbonyolításával" keletkezik.

3.4.5. Lemma [Második Gauss Lemma]. *Tegyük fel, hogy az $f \neq 0$ egész együtthatós polinomot felbontottuk a racionális együtthatós g és h polinomok szorzatára. Ekkor g és h megszorozható alkalmas racionális számokkal úgy, hogy a kapott g_0 és h_0 polinomok egész együtthatósak legyenek, és $f = g_0 h_0$ teljesüljön.*

Bizonyítás. Írjuk föl a g és h polinomokat rg_1 és sh_1 alakban, ahol r, s racionális számok, g_1 és h_1 egész együtthatós primitív polinomok. Ekkor $f = (rs)(g_1 h_1)$. Az első Gauss-lemma első következménye miatt $g_1 h_1$ primitív polinom, a második következménye miatt tehát $n = rs$ egy egész együtthatós polinom, azaz egész szám. Így a $g_0 = ng_1$ és $h_0 = h_1$ választás megfelel a követelményeknek. □

3.4.6. Tétel. *Egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ fölött, ha*

(1) *vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),*
(2) *vagy egy (nem konstans) primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.*

Bizonyítás. A $\mathbb{Z}$-beli felbonthatatlan számokról láttuk, hogy mint konstans polinomok szintén felbonthatatlanok. Tegyük fel, hogy f nem konstans primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis. Ha $f = gh$ egy felbontás, ahol $g, h \in \mathbb{Z}[x]$, akkor a $\mathbb{Q}$ fölötti irreducibilitás miatt g és h egyike egység $\mathbb{Q}$-ban, vagyis konstans, és így egész szám (hiszen g és h egész együtthatós). Mivel f primitív, ez az egész szám csak egység lehet, és így az $f = gh$ felbontás $\mathbb{Z}[x]$-ben is triviális. Tehát f irreducibilis $\mathbb{Z}$ fölött.

Megfordítva, tegyük fel, hogy f irreducibilis polinom $\mathbb{Z}[x]$-ben. Ekkor f felírható nk alakban, ahol n egész szám, és k primitív polinom. Mivel f irreducibilis, ez a felbontás triviális. Így vagy n egység (és akkor f primitív), vagy k egység (és akkor f konstans).

Ha f konstans, akkor nyilván felbonthatatlannak kell lennie $\mathbb{Z}$-ben, hiszen a $\mathbb{Z}$-beli nemtriviális felbontások egyben $\mathbb{Z}[x]$-beli nemtriviális felbontások is. Ha f nem konstans primitív polinom, akkor meg kell mutatnunk, hogy nemcsak $\mathbb{Z}$, hanem $\mathbb{Q}$ fölött is irreducibilis.

Tegyük fel, hogy f előáll a nála alacsonyabb fokú, racionális együtthatós g és h polinomok szorzataként. A második Gauss-lemma miatt ekkor f felírható $g_0 h_0$ alakban is, ahol ezek már egész együtthatós polinomok, és g_0 foka megegyezik g fokával, h_0 foka pedig h fokával. Tehát f_0 és g_0 egyike sem konstans, és így ez nemtriviális felbontás $\mathbb{Z}$-ben is, ami ellentmond f irreducibilitásának $\mathbb{Z}$ fölött. □

Az alaptétel bizonyításához már csak egy észrevételre van szükség.

3.4.7. Állítás. *A $\mathbb{Z}[x]$ gyűrű minden irreducibilis elme prímtulajdonságú.*

Bizonyítás. Az előző tétel miatt ez az irreducibilis elem vagy egy konstans $\mathbb{Z}$-beli prím, vagy egy primitív f polinom, amely $\mathbb{Q}$ fölött irreducibilis. Az első esetben az első Gauss-lemma pont az állítást mondja ki. A második esetben tegyük fel, hogy f osztója $\mathbb{Z}[x]$-ben a gh szorzatnak, ahol g és h egész együtthatós polinomok. Mivel $\mathbb{Q}[x]$-ben igaz az alaptétel, f prímtulajdonságú $\mathbb{Q}[x]$-ben, tehát f osztója g-nek vagy h-nak $\mathbb{Q}[x]$-ben. Az első Gauss-lemma második következménye miatt ez az oszthatóság $\mathbb{Z}[x]$-ben is fönnáll. Így f tényleg prímtulajdonságú. □

3.4.8. Tétel. *A $\mathbb{Z}[x]$ gyűrűben érvényes a számelmélet alaptétele.*

Bizonyítás. Az alaptétel egyértelműségi állítása következik abból, hogy a felbonthatatlan elemek prímtulajdonságúak (lásd 3.1.18. Feladat). Azt kell tehát csak megmutatni, hogy minden f egész együtthatós polinom, amely nem nulla és nem egység, felbontható irreducibilisek szorzatára. Az f polinomot felírhatjuk egy n egész szám és egy g primitív polinom szorzataként, és az n számot felbonthatjuk $\mathbb{Z}$-ben felbonthatatlanok szorzatára, ezek a tényezők $\mathbb{Z}[x]$-ben is felbonthatatlanok lesznek. Tehát elég azt megmutatni, hogy $\mathbb{Z}[x]$ minden primitív, nem konstans g polinomja felírható irreducibilisek szorzataként.

Tegyük fel, hogy ez az állítás nem igaz, legyen g minimális fokú ellenpélda. Ha g maga irreducibilis, akkor önmaga, mint egytényezős felbontás megfelelő lesz. Ha nem, akkor $g = hk$ alakban írható, ahol k és h egyike sem egység. Mivel g primitív, a h és k is primitív polinomok. Így egyikük sem lehet konstans (mert akkor egység lenne), és ezért mindketten g-nél alacsonyabb fokúak. Mivel g foka minimális volt, h és k már felbomlik irreducibilisek szorzatára, de akkor ezt a két felbontást összeszorozva g-t is felbontottuk irreducibilisek szorzatára. Ez az ellentmondás bizonyítja a tételt. □

Az eddigiektől vérszemet kapva megkérdezhetjük, alaptételes-e a $\mathbb{Z}[x, y]$ vagy a $\mathbb{Q}[x, y]$ polinomgyűrű. A válasz igenlő, és a meglepő az, hogy ezt lényegében már be is bizonyítottuk! Például $\mathbb{Q}[x, y]$ úgy tekinthető, mint $\mathbb{Q}[y][x]$, ahol $\mathbb{Q}[y]$-ról tudjuk, hogy alaptételes gyűrű. Ha a most elhangzott bizonyítást el tudnánk mondani $\mathbb{Z}$ helyett $\mathbb{Q}[y]$-ra is, akkor készen lennénk.

Azt kell megvizsgálni, hogy a fenti bizonyításban a $\mathbb{Z}$ milyen tulajdonságait használtuk, és ezek teljesülnek-e $\mathbb{Q}[y]$-ban is. Az alaptételt sokszor, de az $\mathbb{Q}[y]$-ban is teljesül. Használtuk a $\mathbb{Z}_p$ fogalmát is, de csak egy második bizonyításban, tehát ezt nem muszáj általánosítanunk. (Ennek ellenére ez lehetséges, az új fogalmat *faktorgyűrű* néven vezetjük majd be.) Amiről még rengeteget beszéltünk, azok a racionális számok, vagyis a $\mathbb{Z}$ elemeiből készített törtek. De probléma ezzel sincs, hiszen olyan törtekről, amiben az y is szerepel, a középiskolában is sok szó esett, egyenletrendezés kapcsán számoltunk ilyenekkel, bár nem definiáltuk őket pontosan (ezeket, tehát két polinom hányadosát *racionális törtfüggvényeknek* hívják). A *hányadostestről* szóló szakaszban precízen be fogjuk bizonyítani, hogy bármilyen szokásos gyűrű esetében használhatjuk a törteket a szokásos tulajdonságokkal.

Mindezt megelőlegezve, az eddigiek gondos áttanulmányozásával láthatjuk, hogy valójában a közvetkező tételt bizonyítottuk be.

3.4.9. Tétel. *Ha R alaptételes (szokásos) gyűrű, akkor az $R[x]$ polinomgyűrűben is érvényes a számelmélet alaptétele.*

Ezt az áttanulmányozást természetesen csak a hányadostest pontos fogalmának ismeretében lesz majd érdemes elvégezni. Mindenesetre az algebrai szemléletmód erejét mutatja, hogy az alábbi állítás bizonyításához most már a kisujjunkat sem kell mozdítanunk: n szerinti teljes indukcióval azonnal következik az előző tételből.

3.4.10. Következmény. *A $\mathbb{Z}[x_1, \ldots, x_n]$, továbbá tetszőleges T test esetén a $T[x_1, \ldots, x_n]$ gyűrű is alaptételes.*

Gyakorlatok, feladatok

3.4.3. Gyakorlat. Bontsuk $\mathbb{Z}$ fölött irreducibilisek szorzatára a $30x^3 - 30$ polinomot.

3.4.4. Gyakorlat. Mutassuk meg, hogy ha R szokásos gyűrű, és $R[x]$ alaptételes, akkor az R gyűrű is az.

3.4.5. Gyakorlat. Adjunk második bizonyítást arra a tényre, hogy $\mathbb{Z}$ fölött minden polinom irreducibilisek szorzatára bontható úgy, hogy egy $\mathbb{Q}$ fölötti felbontásból indulunk ki, és azt módosítjuk.

3.4.6. Gyakorlat. Bizonyítsuk be, hogy az $f, g \in \mathbb{Z}[x]$ polinomok $\mathbb{Z}[x]$-beli legnagyobb közös osztója a következő eljárással határozható meg. Alkalmazzuk az euklideszi algoritmust $\mathbb{Q}$ fölött, és a kapott racionális együtthatós polinomot írjuk fel rh alakban, ahol $r \in \mathbb{Q}$ és $h \in \mathbb{Z}[x]$ primitív polinom. Határozzuk meg f és g együtthatóinak a közös legnagyobb közös osztóját, ez legyen n. Ekkor f és g legnagyobb közös osztója nh. Hogyan módosítható ez az eljárás, ha két $\mathbb{C}[x, y]$-beli polinom legnagyobb közös osztóját keressük?

3.4.7. Gyakorlat. Mutassuk meg, hogy minden test alaptételes gyűrű. A 3.4.9. Tétel szerint ekkor $T[x]$ is alaptételes. Második bizonyítást kaptunk-e ezzel arra, hogy test fölötti polinomgyűrű alaptételes?

3.5. Irreducibilitás a racionális számtest fölött

A komplex és a valós test fölött át tudtuk tekinteni az összes irreducibilis polinomot, az egész számok gyűrűje fölötti irreducibilitást pedig visszavezettük a racionális számtest fölötti irreducibilitás kérdésére. A racionális számok fölött akárhányadfokú irreducibilis polinomok léteznek, és egy adott polinomról egyáltalán nem könnyű megállapítani, hogy irreducibilis-e, vagy sem. Az irreducibilitás eldöntésére létezik hatékony algoritmus mind $\mathbb{Q}$, mind a véges testek fölött (és így például a `Maple` program meg tudja mondani egy-egy konkrét polinomról, hogy irreducibilis-e), de ennek tárgyalása messze meghaladná e könyv kereteit. Mindössze egy olyan feltételt ismertetünk, amivel, ha szerencsénk van, egy-egy konkrét polinomról megállapíthatjuk, hogy irreducibilis. Ez elegendő lesz a későbbi alkalmazásokhoz is. A bizonyításban használni fogjuk az alábbi segédállítást.

3.5.1. Gyakorlat. Legyen T test, és $r \neq 0$ egy eleme. Mutassuk meg, hogy az rx^n polinom osztói $T[x]$-ben pontosan az sx^m alakú polinomok, ahol $0 \neq s \in T$ és $m \leq n$.

3.5.1. Tétel [A Schönemann-Eisenstein irreducibilitási kritérium]. *Legyen f egy egész együtthatós nem konstans polinom.* ***Ha*** *létezik olyan p prímszám, amelyre*

(1) *p nem osztja f főegyütthatóját;*
(2) *p osztja f összes többi együtthatóját;*
(3) *p^2 nem osztja f konstans tagját,*

akkor *f irreducibilis $\mathbb{Q}$ fölött.*

Mielőtt az állítást bebizonyítanánk, néhány fontos megjegyzést teszünk.

(1) Az állítás megfordítása nem igaz! Például az $x + 1$ polinom irreducibilis $\mathbb{Q}$ fölött, de nincs hozzá megfelelő p prímszám. Tehát ez a kritérium nem ad eljárást az irreducibilitás eldöntésére: ha alkalmazható, akkor a polinom irreducibilis, de ha nem alkalmazható, akkor az irreducibilitást nem tudjuk, és új ötlet után kell néznünk.
(2) Az állítás egész együtthatós polinomokról szól ugyan, de racionális együtthatós polinomokra is alkalmazható lehet, ha a nevezőkkel felszorzunk.
(3) Vigyázzunk: ez a kritérium csak $\mathbb{Q}$ fölötti (és nem $\mathbb{Z}$ fölötti) irreducibilitást biztosít. Például a $9x + 18$ polinomra érvényes a feltétel (ha $p = 2$), és ez a polinom irreducibilis is $\mathbb{Q}$ fölött, de nem irreducibilis $\mathbb{Z}$ fölött (hiszen nem primitív).
(4) A kritérium alapján láthatjuk, hogy az $x^n - 2$ polinom irreducibilis $\mathbb{Q}$ fölött (és így $\mathbb{Z}$ fölött is, hiszen primitív). Vagyis tényleg van akármilyen fokú irreducibilis polinom $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Bizonyítás. Az első Gauss-lemma (3.4.2. Lemma) bizonyításánál először egy együtthatókkal való számolást mutattunk be, majd ennek elemzésével rájöttünk, hogy a polinom modulo p vizsgálatával a számolás elkerülhető. Most fordítva járunk el: a számolásmentes bizonyítást mutatjuk be, és az olvasót a 3.5.2. Gyakorlatban kérjük meg arra, hogy ezt a bizonyítást fordítsa le elemi számolásra. Ha valakinek a modulo p gondolkodás még nehézséget okoz, az megteheti, hogy a Schönemann-Eisenstein kritérium bizonyításaként előbb ennek a gyakorlatnak a megoldását olvassa el.

Tegyük fel tehát, hogy az f polinom és a p prímszám teljesítik a feltételeket, de f mégsem irreducibilis $\mathbb{Q}$ fölött, vagyis az f-nél alacsonyabb fokú, racionális együtthatós g és h polinomok szorzatára bontható. A második Gauss-lemma (3.4.5. Lemma) miatt feltehetjük, hogy g és h egész együtthatós.

Vegyük az f, g, h polinomokat (tehát az együtthatóikat) modulo p, a kapott polinomokat jelölje $\overline{f}$, $\overline{g}$ és $\overline{h}$. Ekkor $\overline{fg} = \overline{f}\ \overline{g}$ (a 2.3.4. Gyakorlat miatt). Ha f főtagja $a_n x^n$, akkor, mivel f többi együtthatója p-vel osztható, az $\overline{f}$ polinom $\overline{a_n}x^n$ lesz (ahol $\overline{a_n} \neq 0$ az a_n maradéka modulo p). Az előző, 3.5.1. Gyakorlat miatt $\overline{a_n}x^n$ minden osztója sx^m alakú alkalmas $s \in \mathbb{Z}_p$-re és $m \leq n$ egészre. Speciálisan

$$\overline{g}(x) = ux^k \quad \text{és} \quad \overline{h}(x) = vx^\ell$$

alkalmas $u, v \in \mathbb{Z}_p$-re. Mivel $\mathbb{Z}_p$ nullosztómentes, a $\overline{g}$ és a $\overline{h}$ fokainak összege az $\overline{f}$ foka, vagyis $k + \ell = n$. De $k = \mathrm{gr}(\overline{g}) \leq \mathrm{gr}(g)$, hiszen ha a g polinomot modulo p vesszük, akkor foka nem nőhet (akkor csökkenhetne, ha a főegyütthatója osztható lenne p-vel). Hasonlóképpen látjuk, hogy $\ell \leq \mathrm{gr}(h)$. Mivel f-et eredetileg két alacsonyabb fokú polinom szorzatára bontottuk fel, k és ℓ mindketten n-nél kisebbek, és mivel összegük n, egyikük sem lehet nulla. Ez azt jelenti, hogy $\overline{g} = ux^k$ konstans tagja nulla, vagyis g konstans tagja osztható p-vel, és ugyanígy h konstans tagja is osztható p-vel. De akkor f konstans tagja, amely g és h konstans tagjainak a szorzata, osztható p^2-tel. Ez ellentmond a feltételeknek. □

3.5.2. Gyakorlat. A fenti gondolatmenetet elemezve adjunk a Schönemann-Eisenstein kritériumra olyan elemi bizonyítást, ami nem használja a $\mathbb{Z}_p[x]$ polinomgyűrűt.

Vigyázzunk, azzal a technikával, hogy „vegyük a felbontást modulo p", óvatosan kell bánni! Például megtörténhet, hogy egy nemtriviális felbontás triviálissá válik mod p. A következő gyakorlatban összefoglaltunk néhány lehetséges anomáliát.

3.5.3. Gyakorlat. Legyen p egy prímszám, $f \in \mathbb{Z}[x]$ egy n-edfokú polinom, ahol $n \geq 1$, és $0 < k < n$. Legyen $\overline{f} \in \mathbb{Z}_p[x]$ az f modulo p véve. Az alábbi állítások közül melyek igazak?

(1) Ha f irreducibilis $\mathbb{Z}$ fölött, akkor $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött.
(2) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, akkor f irreducibilis $\mathbb{Q}$ fölött.
(3) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, és $\overline{f}$ foka n, akkor f irreducibilis $\mathbb{Z}$ fölött.
(4) Ha $\overline{f}$ irreducibilis $\mathbb{Z}_p$ fölött, és $\overline{f}$ foka n, akkor f irreducibilis $\mathbb{Q}$ fölött.
(5) Ha f-nek van $\mathbb{Z}$ fölött k-adfokú tényezője, akkor $\overline{f}$-nak is van k-adfokú tényezője.
(6) Az előző állítás akkor, ha azt is tudjuk, hogy $\overline{f}$ foka n.

Néha előfordul, hogy a Schönemann-Eisenstein kritérium közvetlenül nem alkalmazható, de egy kis átalakítás után igen. Például legyen $f(x) = x^4 + 1$, és számítsuk ki az $f(x+1)$ polinomot:

$$f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2\,.$$

Itt $p = 2$-vel már alkalmazható a kritérium, tehát $f(x+1)$ irreducibilis. De akkor f is az lesz, a következő gyakorlat állítása miatt.

3.5.4. Gyakorlat. Legyen f racionális együtthatós polinom. Mutassuk meg, hogy f akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha valamelyik eltoltja (vagyis az $f(x+c)$ polinom alkalmas $c \in \mathbb{Q}$-ra) irreducibilis $\mathbb{Q}$ fölött. Érvényes marad az állítás más testek fölött is? Mi a helyzet, ha az $x \to x + c$ helyettesítés helyett az $x \to ax + b$ helyettesítést hajtjuk végre, ahol $a \neq 0$?

3.5.5. Feladat. Legyen p prímszám és $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Mutassuk meg, hogy $f(x+1)$ teljesíti a Schönemann-Eisenstein kritérium feltételeit a p prímre, és így f irreducibilis $\mathbb{Q}$ fölött.

A következő gyakorlatban egy másik esetet látunk, amikor a polinom mod p vizsgálata segít az irreducibilitás eldöntésében.

3.5.6. Gyakorlat. Mutassuk meg, modulo 3 vizsgálódva, hogy $6x^4 + 3x + 1$ irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Vegyük észre, hogy noha az előző gyakorlatban szereplő $f(x) = 6x^4+3x+1$ polinomra nem alkalmazható a Schönemann-Eisenstein kritérium, de ha f együtthatóit fordított sorrendben írjuk fel, akkor a kapott polinomra már igen. Ebből már következik az irreducibilitás, ennek megmutatása az előző gyakorlat megoldásának egyszerű általánosítása.

3.5.7. Gyakorlat [A fordított Schönemann-Eisenstein kritérium]. Tegyük föl, hogy f egy egész együtthatós, nem konstans polinom. Igazoljuk, hogy ha létezik olyan p prímszám, amelyre

(1) p nem osztja f konstans tagját;
(2) p osztja f összes többi együtthatóját;
(3) p^2 nem osztja f főegyütthatóját,

akkor f irreducibilis $\mathbb{Q}$ fölött.

A fordított Schönemann-Eisenstein kritérium egy másik bizonyításának is tekinthető az úgynevezett reciprok polinomokról szóló alábbi állítás.

3.5.8. Feladat. Legyen T test, és $f(x) = a_0 + a_1x + \cdots + a_nx^n \in T[x]$, ahol a_0 és a_n nem nulla. Legyen $g(x) = a_n + a_{n-1}x + \cdots + a_0x^n$. Mutassuk meg, hogy

(1) A g polinom T-beli gyökei pontosan az f gyökeinek a reciprokai (multiplicitással számolva is).
(2) Az f akkor és csak akkor irreducibilis T felett, ha g az.

A g polinomot az f-hez tartozó *reciprok polinomnak* is nevezzük. Szokás azt is mondani, hogy f reciprok polinom, ha a hozzá tartozó reciprok polinom maga az f.

Még egy példát mutatunk arra, hogy egy polinom mod p és $\mathbb{Z}$ fölötti felbontásainak együttes vizsgálata hogyan döntheti el az irreducibilitás kérdését.

3.5.2. Példa. Mutassuk meg, hogy $f(x) = x^4 + x^2 + x + 1$ irreducibilis $\mathbb{Q}$ fölött.

Az f polinomot $\mathbb{Z}_2$ fölött szorzatra lehet bontani, az eredmény $(x+1)(x^3+x^2+1)$. Az $x^3 + x^2 + 1$ irreducibilis $\mathbb{Z}_2$ fölött, hiszen harmadfokú, és nincsen $\mathbb{Z}_2$-ben gyöke. Vagyis a polinomunk $\mathbb{Z}_2$ fölött egy elsőfokú és egy harmadfokú irreducibilis szorzata lesz, és a felbontás egyértelműsége miatt $\mathbb{Z}_2$ fölött nem lehet két másodfokú polinom szorzatára bontani. Ezek szerint f-et $\mathbb{Z}$ fölött sem lehet két másodfokú szorzatára bontani (hiszen ha lenne ilyen felbontás, akkor azt vehetnénk modulo 2). Ha tehát $\mathbb{Z}$ fölött f nem irreducibilis, akkor csak egy első- és egy harmadfokú szorzatára lehet bontható. Az elsőfokú tényező racionális gyököt jelentene, ilyen azonban a racionális gyökteszt szerint nincsen (az 1 és a -1 ugyanis nem gyök). Ezért f irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Végül egy utolsó módszert mutatunk az irreducibilitás eldöntésére. Azért hagytuk a végére, mert csak ritkán alkalmazható, általában nagyon bonyolult számolásra vezet. A módszer abban áll, hogy a polinomot általános együtthatókkal bontjuk szorzatra, a szorzást elvégezve pedig az együtthatók összehasonlításával egy egyenletrendszert kapunk. Ennek az egyenletrendszernek a megoldásában néha számelméleti megfontolások is segítenek.

Példaként ismét a fenti $f(x) = x^4 + x^2 + x + 1$ polinomot választjuk. Ennek nincs racionális gyöke, tehát ha felbomlik, akkor csak két másodfokú polinom szorzat lehet:

$$x^4 + x^2 + x + 1 = (ax^2 + bx + c)(ux^2 + vx + w)\,,$$

ahol a, b, c, u, v, w-ről (a második Gauss-lemma miatt) feltehetjük, hogy egész számok. Beszorozva, és az együtthatókat összehasonlítva a következő egyenletrendszert kapjuk:

$$au = 1\,,\ av + bu = 0\,,\ aw + bv + cu = 1\,,\ bw + cv = 1\,,\ cw = 1\,.$$

Szerencsére ezt az egyenletrendszert könnyű megoldani. Mivel $au = 1$, csak $a = u = 1$ vagy $a = u = -1$ lehetséges, ahonnan a második egyenletből $v + b = 0$. Hasonlóképpen az utolsó két egyenletből $c = w = b + v = 1$ vagy $c = w = b + v = -1$ adódik, és ez lehetetlen, mert $b + v = 0$.

3.5.9. Gyakorlat. Felbonthatatlan-e $\mathbb{Z}[x]$-ben az $x^4 + x + 1$ polinom?

Néhány módszer az irreducibilitás eldöntésére $\mathbb{Q}$ és $\mathbb{Z}$ fölött

(1) Egy nem konstans polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ fölött, ha irreducibilis $\mathbb{Q}$ fölött, és primitív.
(2) Ha egy egész együtthatós nem konstans polinom reducibilis $\mathbb{Q}$ fölött, akkor két alacsonyabb fokú *egész együtthatós* polinom szorzatára is felbontható.
(3) Ha egy legalább másodfokú polinomnak van racionális gyöke, akkor nem irreducibilis $\mathbb{Q}$ fölött. Egy másod- vagy harmadfokú polinom pontosan akkor irreducibilis $\mathbb{Q}$ fölött, ha nincs racionális gyöke (használjuk a racionális gyöktesztet). A racionális gyökök az elsőfokú tényezőknek felelnek meg.
(4) Bontsuk föl a polinomot $\mathbb{C}$ vagy $\mathbb{R}$ fölött, és használjuk a felbontás egyértelműségét (lásd a 3.3.10. Példát).
(5) A (fordított) Schönemann-Eisenstein kritérium.
(6) Egy $f \in \mathbb{Q}[x]$ polinom akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha egy eltoltja ($f(x + c)$, $c \in \mathbb{Q}$) az.
(7) Ha $f \in \mathbb{Z}[x]$, akkor vizsgáljuk modulo p, ahol p prímszám.
(8) Bontsuk föl a polinomot általános együtthatókkal, és oldjuk meg a kapott egyenletrendszert.
(9) Az úgynevezett *körosztási polinomok* irreducibilisek (ezekről a 3.9. Szakaszban lesz szó).
(10) Negyedfokú polinom esetében vizsgálhatjuk az úgynevezett harmadfokú rezolvenst (lásd 3.8.4. Feladat).

E módszereknek sokszor a kombinációja az, ami célhoz vezet. Az alábbi feladatokban néha csak annyi a nehézség, hogy megtaláljuk, milyen irányba induljunk el.

Gyakorlatok, feladatok

3.5.10. Gyakorlat. Az alább felsorolt polinomok közül melyekre alkalmazható közvetlenül a Schönemann-Eisenstein kritérium: $x^{11}+2x+18$, $x^{11}+2x+12$, $x^{11}+12x+5$, $x^{11}+24$, $x^{11}+72$. Mely n egészekre felel meg az $x^{11}+n$ polinom?

3.5.11. Gyakorlat. Irreducibilisek-e az alábbi polinomok?

(1) $\mathbb{C}$, illetve $\mathbb{R}$ fölött x^7+x+1, x^2-2, x^2+x+1.
(2) $\mathbb{Q}$ fölött $3x^7-6x^6+6x^2+3x-2$, $3x^7+x^6+6x^2+2x-2$, $3x^7-6x^6+6x^2+2x-2$, $x^{16}+1$, $x^{16}+2$, x^4-14x^2+9, x^4-x^2+1, $3x^7+6x-18$, x^5+4, x^3+9, x^3+3, $x^{10}-x^5+1$, $x^{10}+10$, x^4+25, x^4+2, x^4+4x+1, x^4-2x+1, $2x^4+2x^2+1$, $x^6-10x+10$, $x^4+x^3+x^2+1$.
(3) $\mathbb{Z}$ fölött $x^4+2x+27$, $3x^7+6x-18$, x^6+1, x^3+7x-3, $x^4+3x^3+x^2+1$.

3.5.12. Feladat. Van-e olyan $f(x)$ egész együtthatós polinom, hogy minden $g(x)$ egész együtthatós, nem konstans polinomra az $f\big(g(x)\big)$ polinom irreducibilis legyen $\mathbb{Q}$ fölött?

3.5.13. Feladat. Legyen $f(x,y)=x^9+x^3y^3+y^2+y\in\mathbb{C}[x,y]$, és jelölje $\mathbb{C}(y)$ az $f(y)/g(y)$ alakú racionális törtfüggvényekből álló testet ($f,g\in\mathbb{C}[y]$).

(1) Primitív-e f, mint $\mathbb{C}[y]$ fölötti polinom?
(2) Következik-e a Schönemann-Eisenstein tételből, hogy f irreducibilis $\mathbb{C}(y)$ fölött?
(3) Irreducibilis-e f a $\mathbb{C}[x,y]$-ban?

3.5.14. Feladat. Annak felhasználásával, hogy x^3-2 irreducibilis $\mathbb{Q}$ fölött, mutassuk meg, hogy $\sqrt[3]{4}$ nem írható fel $a+b\sqrt[3]{2}$ alakban, ahol a és b racionális számok.

3.6. A derivált és a többszörös gyökök

Aki tanult már analízist, az ismerheti a differenciálszámítás rendkívül hasznos apparátusát. Ha egy függvény, például a valós együtthatós

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

polinomhoz tartozó polinomfüggvény maximumát vagy minimumát akarjuk meghatározni, akkor elkészítjük ennek a függvénynek az úgynevezett *deriváltját*, amely a következő lesz:

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1\,.$$

A derivált gyökei szoros kapcsolatban állnak az eredeti függvény szélsőértékeivel.

Mi nem a szélsőértékeket, hanem az f polinom többszörös gyökeit szeretnénk megkeresni. A derivált fogalma ehhez is segítséget nyújt, mert *az f többszörös gyökei a deriváltjának is gyökei lesznek.* Ahhoz, hogy ezt az állítást beláthassuk, a polinomot gyöktényezős

alakban kellene felírni, és így deriválni. Szükségünk lenne tehát egy szabályra, amely megmondja, hogy szorzatot hogyan kell deriválni. Az analízis ebben is a segítségünkre van, hiszen az ismert Leibniz-szabály szerint

$$(fg)' = f'g + fg'$$

teljesül tetszőleges f és g polinomfüggvényekre (sőt általában differenciálható függvényekre is). Ennek alapján például ha f-nek az 1 legalább háromszoros gyöke, vagyis ha

$$f(x) = (x-1)^3 g(x)\,,$$

akkor

$$f'(x) = \big((x-1)^3\big)' g(x) + (x-1)^3 g'(x)\,.$$

Könnyű látni, hogy $(x-1)^3$ deriváltja $3(x-1)^2$, és így f'-ből kiemelhető $(x-1)^2$. Vagyis az 1 szám az f deriváltjának legalább kétszeres gyöke lesz.

Nagyon fontos észrevennünk a következőt. A deriváltat ugyan folytonossági megfontolásokkal származtatják, de a fenti gondolatmenetben a deriválásnak csak a számolási szabályait használtuk! Reménykedhetünk hát, hogy a fenti számolást ki lehet terjeszteni a valós helyett például véges testekre is, ahol a folytonossági megfontolások hasznavehetetlenek, de a számolási szabályok esetleg érvényesek maradnak. Így apparátust kapnánk tetszőleges test fölött a többszörös gyökök vizsgálatára. Most ezt az ötletet fogjuk kivitelezni.

3.6.1. Definíció. Legyen R szokásos gyűrű, és

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

egy $R[x]$-beli polinom. Ekkor f *formális deriváltján* az

$$f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

polinomot értjük.

Láthatjuk, hogy immáron nem a polinomfüggvényeket, hanem magukat a polinomokat deriváljuk. A képletben szereplő együtthatókat, például na_n-et úgy kell érteni, hogy az a_n elemet n példányban önmagával összeadjuk (egy gyűrűelem egész számszorosát a 2.2.8. Definícióban, illetve az azt követő megjegyzésekben értelmeztük, amikor a hatvány, illetve többszörös általános fogalmáról volt szó).

3.6.2. Állítás. *Ha R szokásos gyűrű, akkor tetszőleges $f, g \in R[x]$ polinomokra érvényesek az alábbi deriválási szabályok.*

(1) $(f+g)' = f' + g'$.
(2) $(fg)' = f'g + fg'$, *speciálisan* $(cf)' = cf'$ *minden* $c \in R$ *esetén (hiszen* $c' = 0$*).*
(3) $f\big(g(x)\big)' = f'\big(g(x)\big)g'(x)$ *(láncszabály).*

Ezeknek a szabályoknak az igazolása úgy történhet, hogy az f és g polinomokat általános együtthatókkal írjuk fel, és a bizonyítandó azonosság mindkét oldalát kiszámoljuk. A számolásban néha segít, ha f vagy g foka szerinti indukciót alkalmazunk. A részletek kidolgozását az olvasóra hagyjuk.

Az igazi matematikust nem elégíti ki, ha a fenti szabályokat számolással kihozza, tudni szeretné azt is, hogy ezek az analízisben tanult (és az ottani módszerekkel sokkal elegánsabban bizonyított) szabályok miért maradnak meg tetszőleges gyűrű fölött is. Egy lehetséges magyarázat szerepel Fried Ervin [**5**] könyvében (I. rész, 4.3. Fejezet). Röviden a következőről van szó.

Amikor a deriváltat képezzük, akkor az f függvény görbéjét egy rögzített b pont kis környezetében egy $y = cx + d$ egyenessel akarjuk közelíteni (és $f'(b)$ ennek az egyenesnek az iránytangense, vagyis c lesz). Azt akarjuk, hogy a kettő „egymáshoz simuljon". Ha például $b = 0$, akkor

$$f(x) - (cx + d)$$

kell, hogy „kis" x-ekre az x-hez képest „nagyon kicsi" legyen. Ha

$$f(x) = a_0 + a_1x + a_2x^2 + \dots ,$$

akkor

$$f(x) - (cx + d) = (a_0 - d) + (a_1 - c)x + a_2x^2 + \dots .$$

Ez akkor lesz „elég kicsi" x-hez képest, ha $a_0 = d$ és $a_1 = c$, vagyis ha ebben a különbségben már csak csupa x^2-tel osztható tag szerepel (ez az egyenessel elérhető legjobb közelítés). Ezért lesz tehát $f'(0) = a_1$.

Ha a b pont tetszőleges, akkor a változót $b + x$ alakban érdemes felírni, tehát a fenti képlet úgy módosul, hogy az

$$f(b + x) - \big(c(b + x) + d\big)$$

kifejezésről (mint x polinomjáról) követeljük meg, hogy „kis" x-ekre az x-hez képest „nagyon kicsi" legyen, azaz hogy ne legyen benne se konstans tag, se x-es tag, vagyis osztható legyen x^2-tel. Innen ismét kiszámítható az $f'(b) = c$ értéke. Ez már tisztán algebrai átfogalmazás, hiszen nincsen benne szó közelítésről, kicsi és nagy számokról, hanem csak polinomok oszthatóságáról, és így elmondható általános gyűrű fölött is. Az érdeklődő olvasó Fried Ervin idézett könyvében elolvashatja, hogy ez az átfogalmazott definíció hogyan vezet el a deriválás: tulajdonságainak elegáns bizonyításához.

3.6.3. Állítás. *Legyen R szokásos gyűrű, $b \in R$, és tegyük fel, hogy b az $f \in R[x]$ polinomnak legalább k-szoros gyöke. Ekkor b az f deriváltjának legalább $k - 1$-szeres gyöke.*

Bizonyítás. Ez a már bemutatott számolás könnyű általánosítása. Mivel b legalább k-szoros gyök, f felírható

$$f(x) = (x - b)^k q(x)$$

alakban, ahol $q \in R[x]$. Deriválva

$$f'(x) = \big((x - b)^k\big)' q(x) + (x - b)^k q'(x) .$$

A láncszabály szerint $(x - b)^k$ deriváltja $k(x - b)^{k-1}$ (hiszen a belső $x - b$ polinom deriváltja 1). Ezért $(x - b)^{k-1}$ tényleg osztója f deriváltjának. □

A számolást folytatva

$$f'(x) = (x - b)^{k-1}\big[kq(x) + (x - b)q'(x)\big] .$$

Tegyük föl, hogy b pontosan k-szoros gyöke f-nek, azaz $q(b) \neq 0$. A szögletes zárójelben lévő polinomba $x = b$-t helyettesítve a második tag eltűnik, és az eredmény $kq(b)$ lesz. Azt gondolhatnánk, hogy $k \neq 0$ esetén $kq(b)$ sem lesz nulla, és így b pontosan $k-1$-szeres gyöke f'-nek. A valós számok teste fölött ez biztosan így is van. A következő példa azonban óvatosságra int.

Kérdés. Legyen $f(x) = x^3 + x^2$ a $\mathbb{Z}_2$ fölött. Hányszoros gyöke ennek a nulla? És a deriváltjának hányszoros gyöke a nulla?

Válasz: mivel $x^3 + x^2 = x^2(x+1)$ és itt 0 már nem gyöke az $x+1$-nek, ezért a nulla pontosan kétszeres gyök. A polinom deriváltja $3x^2 + 2x$. Itt a 2 együtthatót úgy kell érteni, hogy az x^2 eredeti együtthatóját, ami 1, kétszer összeadjuk önmagával. De a $\mathbb{Z}_2$ testben $1 + 1 = 0$. Ezért f deriváltja $3x^2 = x^2$ lesz. Ennek pedig a nulla szintén kétszeres gyöke!

Érdemes összevetni a fentieket a 3.3.7. Gyakorlat megoldásában fellépő $(x+1)^2 = x^2 + 1$ összefüggéssel. Az $(x+1)^2$ kiszámításakor nem lép fel a 2 szám: az x-es tag együtthatója $1 +_2 1 = 0$ lesz. Ugyanakkor valakinek eszébe juthat, hogy az $(x+1)^2$ kiszámítására a 2.2.17. Gyakorlatban bizonyított binomiális tételt alkalmazza. Ekkor már a fent vizsgált jelenséggel szembesül, nevezetesen, hogy a $\mathbb{Z}_2[x]$ gyűrűben $2x = x + x = 0$.

A probléma oka tehát a következő: egy R nullosztómentes gyűrűben a $kq(b)$ igenis lehet nulla akkor is, ha sem k sem $q(b)$ nem nulla, hiszen k nem gyűrűelem, hanem egész szám! Például $\mathbb{Z}_2$-ben $2 \cdot 1 = 0$, noha a 2 egész szám nem nulla, és az $1 \in \mathbb{Z}_2$ sem nulla! Most már megfogalmazhatjuk azt a feltételt, ami biztosítja, hogy f'-nek a b pontosan $k-1$-szeres gyöke legyen.

3.6.4. Tétel. *Legyen R szokásos gyűrű, $b \in R$, és tegyük fel, hogy b az $f \in R[x]$ polinomnak pontosan k-szoros gyöke ($k \geq 1$ egész). Ekkor b az f deriváltjának legalább $k-1$-szeres gyöke. Ha az R gyűrű tetszőleges r elemére teljesül, hogy $kr = 0$-ból $r = 0$ következik, akkor b az f deriváltjának pontosan $k-1$-szeres gyöke.* □

A tételbeli feltétel teljesül, ha $k = 1$ (és az R gyűrű tetszőleges). Ebben az esetben arról van szó, hogy b a deriváltnak nullaszoros gyöke, vagyis nem gyöke. *Ha tehát egy elem egy polinomnak pontosan egyszeres gyöke, akkor a deriváltjának biztosan nem gyöke.* A feltétel akkor is teljesül, ha R az egész, a racionális, a valós, vagy a komplex számok gyűrűje (és k tetszőleges). Erre a furcsa feltételre vissza fogunk térni később, amikor gyűrűk *karakterisztikájáról* lesz szó.

3.6.5. Következmény. *Legyen R szokásos gyűrű, és $f \in R[x]$. Ekkor az f polinom többszörös gyökei pontosan az f és f' közös gyökei.*

Bizonyítás. Ha $b \in R$ legalább kétszeres gyöke f-nek, akkor gyöke f'-nek is, és így közös gyöke f-nek és f'-nek. Megfordítva, ha b közös gyöke f-nek és f'-nek, akkor f-nek legalább kétszeres gyöke, hiszen ha csak egyszeres gyöke lenne, akkor az előző állítás szerint f'-nek nullaszoros gyöke lenne. □

Ha tehát az az $(f,\ f')$ kitüntetett közös osztó létezik, akkor (a 3.2.6. Állítás szerint) ennek gyökei pontosan f többszörös gyökei. Így például test fölött a többszörös gyököket kereshetjük úgy, hogy az euklideszi algoritmussal kiszámítjuk f és f' kitüntetett közös osztóját. Speciálisan ha $(f,\ f')$ konstans, akkor f-nek nincs többszörös gyöke. Vizsgálhatjuk azt is, hogy van-e f-nek legalább háromszoros, négyszeres, stb. gyöke, ha a második, harmadik, stb. deriváltakat tekintjük (lásd a 3.6.5. Gyakorlatot, és a 3.6.6. Feladatot).

Gyakorlatok, feladatok

3.6.1. Gyakorlat. Határozzuk meg az $x^6+x^5+5x^4+4x^3+8x^2+4x+4$ polinom többszörös komplex gyökeit.

3.6.2. Gyakorlat. Miért igaz, hogy $\mathbb{Z}_2$ fölött $3x^2 = x^2$? Miért nem mondhatjuk ugyanilyen alapon a következőt: „$\mathbb{Z}_2$ fölött $x^2 = x$, hiszen $\mathbb{Z}_2$ bármelyik elemét, azaz akár 0-t, akár 1-et helyettesítünk, az x^2 és az x ugyanazt az értéket veszi föl”?

3.6.3. Gyakorlat. Adjunk meg egy olyan polinomot egy alkalmas test fölött, melynek egy nyolcszoros gyöke a polinom deriváltjának is (pontosan) nyolcszoros gyöke.

3.6.4. Gyakorlat. Legyen f egy $\mathbb{C}$ fölötti polinom, és tegyük fel, hogy f'-nek egy $b \in \mathbb{C}$ szám pontosan $k-1$-szeres gyöke (ahol $k \geq 1$ egész). Igazoljuk, hogy ha b gyöke f-nek, akkor pontosan k-szoros gyöke. Igaz-e ez az állítás tetszőleges test fölött?

3.6.5. Gyakorlat. Mutassuk meg, hogy egy f polinom legalább k-szoros gyökei az f-nek és a $k-1$-edik deriváltjának közös gyökei. Igaz-e az állítás megfordítása?

3.6.6. Feladat. Legyen $f \in \mathbb{Q}[x]$ normált polinom, és $k \geq 1$ egész. Jelölje $g_k(x)$ azoknak az $x-b$ gyöktényezőknek a szorzatát, amelyre $b \in \mathbb{C}$ az f-nek pontosan k-szoros gyöke. Mutassuk meg, hogy g_k is racionális együtthatós.

3.6.7. Gyakorlat. Igazoljuk tetszőleges test fölött, hogy ha egy f polinomnak van többszörös tényezője (azaz g^2 alakú osztója, ahol g nem konstans polinom), akkor $(f,\ f') \neq 1$. Mely p prímekre igaz, hogy x^n-1-nek van többszörös tényezője $\mathbb{Z}_p$ fölött?

3.6.8. Feladat. Lehet-e egy $\mathbb{Q}$, illetve $\mathbb{Z}_2$ fölött irreducibilis polinomnak többszörös gyöke egy nagyobb testben?

3.6.9. Gyakorlat. Legyen $f(x) = c(x-b_1)\dots(x-b_n)$, ahol $c \neq 0$, $b_1, \dots, b_n$ egy T test elemei. Mutassuk meg, hogy

$$f'(x) = \frac{f(x)}{x-b_1} + \dots + \frac{f(x)}{x-b_n},$$

és hogy $f'(b_i) = c(b_i-b_1)\dots(b_i-b_{i-1})(b_i-b_{i+1})\dots(b_i-b_n)$.

3.6.10. Feladat. Mutassuk meg, hogy ha $f \in \mathbb{C}[x]$ legalább másodfokú polinom, akkor van olyan $c \in \mathbb{C}$, melyre $f(x)+c$-nek van többszörös komplex gyöke.

3.6.11. Feladat. Igazoljuk, hogy egy n-edfokú, $\mathbb{C}$ feletti polinom, legfeljebb $n-1$ kivételes értéktől eltekintve, az értékkészletének minden elemét n különböző helyen veszi fel.

3.7. A rezultáns és a diszkrimináns

Noha hasznos ismereteket tartalmaz, ez és a következő szakasz egy kitérő azon az úton, amit ebben a könyvben be szeretnénk járni, nevezetesen, hogy eljussunk az absztrakt algebrai fogalmak mély megértéséhez. Ezért ez a két szakasz vázlatosabb az eddigieknél, és a könyv későbbi részének megértéséhez nem szükséges elolvasni őket. Aki mégis rászánja magát, annak azt javasoljuk, hogy ismételje át a determinánsok alaptulajdonságait, például Freud Róbert [**3**] könyve, és a függelékben található lineáris algebrai összefoglaló alapján.

A 3.2.6. Állítás szerint az f és g polinomok közös gyökeit úgy kereshetjük meg, hogy (például az euklideszi algoritmussal) meghatározzuk a kitüntetett közös osztójukat. Képzeljük el azonban, hogy f és g együtthatói egy t paramétertől függenek, és azt szeretnénk tudni, hogy milyen t értékek azok, amelyekre f-nek és g-nek *van* közös gyöke. Az euklideszi algoritmust ezzel az általános paraméterrel végigszámolni reménytelennek tűnik, és ezért jó lenne, ha föl tudnánk írni egy képletet f és g együtthatói segítségével, amely pontosan akkor nulla, ha f-nek és g-nek van közös gyöke. Ilyen képlet az f és g *rezultánsa*. Ez arra is alkalmas, hogy többismeretlenes egyenletrendszereket egyismeretlenesre vezessünk vissza.

3.7.1. Definíció. Legyen T test, és $f, g \in T[x]$, mégpedig

$$f(x) = a_n x^n + \cdots + a_0 \quad \text{és} \quad g(x) = b_m x^m + \cdots + b_0 \,.$$

Az f és g *rezultánsa* az az $R(f, g)$-vel jelölt $(m + n) \times (m + n)$-es determináns, amit a következőképpen készítünk el. Az első sorba az $a_n, a_{n-1}, \ldots, a_0$ együtthatókat írjuk, majd csupa nullákat. A második sor első eleme nulla, ezután jönnek sorban $a_n, a_{n-1}, \ldots, a_0$, majd ismét csupa nulla. A harmadik sor elején már két nulla van. Ezt a lépcsőt összesen m soron át folytatjuk, ekkor az m-edik sorban a_0 lesz a legutolsó elem. Ezután ugyanezt az eljárást a maradék n sorban elvégezzük a $b_m, b_{m-1}, \ldots, b_0$ együtthatókkal is.

Példaként lássuk ezt a determinánst, amikor $n = 4$ és $m = 3$:

$$R(f, g) = \begin{vmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_4 & a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_4 & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 & 0 & 0 \\ 0 & 0 & b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & 0 & b_3 & b_2 & b_1 & b_0 \end{vmatrix}$$

Annak magyarázata, hogy hogyan jut eszünkbe pont ezt a determinánst felírni, megtalálható Fried Ervin [**5**] könyvében (II. rész, 9.3. Fejezet).

Fontos megjegyeznünk, hogy a rezultáns definíciójában megengedtük azt az esetet is, hogy a_n (vagy b_m) nulla legyen. A rezultáns tehát nemcsak az f és g polinomoktól függ, hanem az n és m számoktól is, azaz attól, hogy hány nulla együtthatót írunk ki a polinom „tetejére". Emiatt a rezultáns $a_n = b_m = 0$ esetén is nulla lesz, nemcsak akkor, amikor

a két polinomnak van közös gyöke. Az olvasó joggal kérdezheti: mi értelme van annak, hogy „felesleges” nulla együtthatókat írjunk a determinánsba?

A válasz a következő: elképzelhető, hogy az a_n és b_m együtthatókról *nem tudjuk,* hogy nullával egyenlőek-e! Ha mondjuk a_n egy t paramétertől függő kifejezés, akkor kényelmetlen (sőt néha kivitelezhetetlen) lenne előbb megvizsgálni, hogy mely t értékekre lesz ez nulla, és attól függően más és más rezultánst fölírni. Sokkal egyszerűbb ezt a determinánst csak egyszer kiszámítani. Erre a jelenségre példát fogunk mutatni, amikor a rezultánst egy egyenletrendszer megoldására alkalmazzuk.

A rezultáns fő tulajdonságát a 3.7.3. Tételben mondjuk ki. A több lehetséges bizonyítás közül azt mutatjuk be, amely nagyon tanulságos absztrakt algebrai szempontból is.

3.7.2. Állítás. *Legyen T test, $f(x) = a_n(x-\alpha_1)\dots(x-\alpha_n)$, ahol $a_n, \alpha_1, \dots, \alpha_n \in T$, és $g(x) = b_m x^m + \dots + b_0 \in T[x]$. Ekkor*

$$R(f,g) = a_n^m g(\alpha_1)\dots g(\alpha_n)\,.$$

Felhívjuk a figyelmet arra, hogy ebben az állításban ($f \neq 0$ esetén) el van rejtve az a feltétel, hogy $a_n \neq 0$ az f főegyütthatója, ugyanakkor $b_m \neq 0$ nincs feltéve.

Bizonyítás. A számolást célszerű úgy elvégezni (a bizonyítás során meglátjuk miért), hogy az α_i, b_j, a_n konkrét T-beli elemek helyett határozatlanokkal számolunk. Ezért tekintsük az $R = T[u, v_0, \dots, v_m, x_1, \dots, x_n, y_1, \dots, y_m]$ polinomgyűrűt, és $R[x]$-ben az

$$F(x) = u(x-x_1)\dots(x-x_n)\,,$$

valamint a

$$G(x) = v_m x^m + \dots + v_0$$

polinomokat. Ha belátjuk, hogy $R(F,G) = u^m G(x_1)\dots G(x_n)$, akkor innen az $x_i \mapsto \alpha_i$, $v_j \mapsto b_j$, $u \mapsto a_n$ helyettesítéssel az állítást kapjuk. Az $y_1, \dots, y_m$ a számolás során használt segédváltozók lesznek.

Az $R(F,G)$ rezultáns definíciójában szerepelő determinánst szorozzuk meg jobbról a $V(y_1, \dots, y_m, x_1, \dots, x_n)$ Vandermonde-determinánssal (lásd D.0.14). A fent bemutatott $n = 4$ és $m = 3$ esetben tehát a következő determinánsról van szó:

$$\begin{vmatrix}
y_1^6 & y_2^6 & y_3^6 & x_1^6 & x_2^6 & x_3^6 & x_4^6 \\
y_1^5 & y_2^5 & y_3^5 & x_1^5 & x_2^5 & x_3^5 & x_4^5 \\
y_1^4 & y_2^4 & y_3^4 & x_1^4 & x_2^4 & x_3^4 & x_4^4 \\
y_1^3 & y_2^3 & y_3^3 & x_1^3 & x_2^3 & x_3^3 & x_4^3 \\
y_1^2 & y_2^2 & y_3^2 & x_1^2 & x_2^2 & x_3^2 & x_4^2 \\
y_1 & y_2 & y_3 & x_1 & x_2 & x_3 & x_4 \\
1 & 1 & 1 & 1 & 1 & 1 & 1
\end{vmatrix}$$

A determinánsok szorzástételét (D.0.15. Tétel) alkalmazzuk, és ezért számítsuk ki a két mátrix szorzatát. Eredményként egy olyan mátrixot kapunk, amely négy részmátrixból

tehető össze. A bal felső sarokban egy $m \times m$-es M mátrix áll, amelyben az i-edik sor j-edik eleme $F(y_j)y_j^{m-i}$. Mellette jobbra egy $m \times n$-es részmátrix áll, melynek elemei $F(x_j)x_j^{m-i}$. Ezek az elemek nullával egyenlőek, hiszen $F(x_j) = 0$ az F definíciója miatt. A bal alsó sarokban egy $n \times m$-es részmátrix áll, melynek elemei $G(y_j)y_j^{n-i}$. Végül a jobb alsó sarokban álló $n \times n$-es N részmátrix elemei $G(x_j)x_j^{n-i}$. Az $n = 4$ és $m = 3$ esetben tehát a következő determinánst kapjuk:

$$\left|\begin{array}{ccc|cccc} F(y_1)y_1^2 & F(y_2)y_2^2 & F(y_3)y_3^2 & F(x_1)x_1^2 & F(x_2)x_2^2 & F(x_3)x_3^2 & F(x_4)x_4^2 \\ F(y_1)y_1 & F(y_2)y_2 & F(y_3)y_3 & F(x_1)x_1 & F(x_2)x_2 & F(x_3)x_3 & F(x_4)x_4 \\ F(y_1) & F(y_2) & F(y_3) & F(x_1) & F(x_2) & F(x_3) & F(x_4) \\ \hline G(y_1)y_1^3 & G(y_2)y_2^3 & G(y_3)y_3^3 & G(x_1)x_1^3 & G(x_2)x_2^3 & G(x_3)x_3^3 & G(x_4)x_4^3 \\ G(y_1)y_1^2 & G(y_2)y_2^2 & G(y_3)y_3^2 & G(x_1)x_1^2 & G(x_2)x_2^2 & G(x_3)x_3^2 & G(x_4)x_4^2 \\ G(y_1)y_1 & G(y_2)y_2 & G(y_3)y_3 & G(x_1)x_1 & G(x_2)x_2 & G(x_3)x_3 & G(x_4)x_4 \\ G(y_1) & G(y_2) & G(y_3) & G(x_1) & G(x_2) & G(x_3) & G(x_4) \end{array}\right|$$

Mivel a jobb felső sarokban álló részmátrix mindegyik eleme nulla, ez a determináns az M és N részmátrixok determinánsainak a szorzata lesz (lásd D.0.16). Az M részmátrix oszlopaiból $F(y_j)$-t kiemelve a $V(y_1, \dots, y_m)$ Vandermonde-determináns marad. Hasonlóan N oszlopaiból $G(x_j)$-t kiemelve $V(x_1, \dots, x_n)$ marad. Mindezt összevetve

$$\begin{aligned} &R(F, G)V(y_1, \dots, y_m, x_1, \dots, x_n) = \\ &\quad = F(y_1) \dots F(y_m)V(y_1, \dots, y_m)G(x_1) \dots G(x_n)V(x_1, \dots, x_n)\,. \end{aligned}$$

Itt $F(y_i) = u(y_i - x_1) \dots (y_i - x_n)$. A Vandermonde-determinánsok kifejtését beírva, és az $y_i - x_j$, $x_i - x_j$, $y_i - y_j$ nem nulla polinomokkal egyszerűsítve pontosan a bizonyítandó összefüggést kapjuk. Ez az egyszerűsítés megengedett, mert az R nullosztómentes (hiszen test fölötti polinomgyűrű). □

Most már világos, hogy miért kellett az α_i helyett határozatlanokkal számolni. Az ugyanis véletlenül megeshet, hogy f-nek van többszörös gyöke, és akkor $\alpha_i - \alpha_j$ nulla is lehet, amivel a fenti bizonyításban nem tudnánk egyszerűsíteni. A megfelelő $x_i - x_j$ polinom azonban nem a nulla polinom. A vele való egyszerűsítés ezért megengedett, és két egyenlő polinomot kapunk az egyszerűsítés után is. Ide helyettesítünk azután az x_i helyébe α_i-t. (Érdemes elolvasni mindezzel kapcsolatban a 2.5.10. Feladat (4)-es pontjának megoldását követő megjegyzéseket.)

3.7.3. Tétel. *Legyenek $f(x) = a_n x^n + \dots + a_0$, valamint $g(x) = b_m x^m + \dots + b_0$ egy T test fölötti polinomok, melyek T fölött gyöktényezőkre bomlanak.*

(1) *Tegyük fel, hogy a_n és b_m egyike sem nulla, és így f és g gyöktényezős alakja felírható $f(x) = a_n(x - \alpha_1) \dots (x - \alpha_n)$ és $g(x) = b_m(x - \beta_1) \dots (x - \beta_n)$*

alakban, ahol α_i, β_j a T test elemei. Ekkor

$$R(f,g) = a_n^m g(\alpha_1)\dots g(\alpha_n) = a_n^m b_m^n \prod_{1\le i\le n}\prod_{1\le j\le m}(\alpha_i-\beta_j) =$$
$$= (-1)^{nm} b_m^n f(\beta_1)\dots f(\beta_m) = (-1)^{nm} R(g,f)\,.$$

(2) *Az $R(f,g)$ akkor és csak akkor nulla, ha vagy $a_n = b_m = 0$, vagy a két polinomnak van közös gyöke T-ben.*

Bizonyítás. Az (1) állítás első egyenlőségét már beláttuk az előző állításban. A második egyenlőség ebből azonnal látszik, ha g gyöktényezős alakjába behelyettesítünk. Ha mindegyik $\alpha_i - \beta_j$ szorzatot megfordítjuk, akkor összesen mn-szer váltottunk előjelet. Az f gyöktényezős alakjából tehát a harmadik egyenlőséget is megkapjuk. Innen az utolsó egyenlőség ismét az előző állításból következik, f és g szerepének megcserélésével.

Bizonyítsuk be most a (2) állítást. Az (1)-ből következik, hogy ha két polinomnak van közös gyöke, akkor a rezultánsuk biztosan nulla. Ha $a_n = b_m = 0$, akkor a rezultáns definíciójában a determináns első oszlopa nulla, és így a rezultáns is nulla. Tegyük fel most, hogy $R(f,g) = 0$. Meg kell mutatni, hogy ha a_n és b_m *valamelyike* nem nulla, akkor f-nek és g-nek van közös gyöke T-ben. Vegyük észre, hogy az $R(f,g) = (-1)^{nm} R(g,f)$ egyenlőség közvetlenül is világos, hiszen a determináns két sor cseréjekor előjelet vált. Ezért $R(g,f) = 0$ is igaz, vagyis f és g szerepe megcserélhető. Így feltehető, hogy $a_n \neq 0$ (mert akkor ugyanez a gondolatmenet f és g cseréje után a $b_m \neq 0$ esetet is elintézi).

Ha $a_n \neq 0$, akkor alkalmazhatjuk a fent bizonyított 3.7.2. Állítást, és azt kapjuk, hogy

$$0 = R(f,g) = a_n^m g(\alpha_1)\dots g(\alpha_n)\,.$$

Mivel $a_n \neq 0$, valamelyik α_i gyöke g-nek, tehát van közös gyök. □

A most bizonyított tétel akkor izgalmas, ha az f és g polinomoknak nem ismerjük a gyökeit. De mi a helyzet akkor, ha például racionális együtthatós polinomokról van szó, amelyeknek nincsen racionális gyöke? Mit mond róluk az, hogy a rezultánsuk nulla? Ebben az esetben a tételt a komplex számtestben érdemes alkalmazni (mert ott minden polinom gyöktényezős alakra bomlik), és azt kapjuk, hogy a két polinomnak van közös komplex gyöke. Később be fogjuk bizonyítani, hogy nemcsak a $\mathbb{Q}$, hanem minden test részteste egy olyan testnek, amelyben már minden polinomnak van gyöke. Ha a tételt erre a bővebb testre alkalmazzuk, akkor az alábbi következményt kapjuk.

3.7.4. Következmény. *Ha T test, akkor a T fölötti $a_n x^n + \dots + a_0$ és $b_m x^m + \dots + b_0$ polinomok rezultánsa akkor és csak akkor tűnik el, ha vagy $a_n = b_m = 0$, vagy a két polinomnak van közös gyöke egy alkalmas T-nél bővebb testben (aminek tehát T részteste).*

A rezultánsnak több alkalmazása is van. A szakasz végén megmutatjuk, hogyan lehet egyenletrendszereket megoldani a segítségével. Hasznos a rezultáns akkor is, ha egy polinom többszörös gyökeit akarjuk vizsgálni. Tudjuk, hogy egy f polinom többszörös gyökei az f-nek és a deriváltjának a közös gyökei, és így az $R(f,f')$ rezultáns akkor lesz nulla,

ha a polinomnak van többszörös gyöke. Látni fogjuk azonban, hogy a következő eredmény akkor is hasznos információt nyújt a gyökökről, ha mindegyik csak egyszeres, például segít megállapítani egy valós együtthatós polinom valós gyökeinek a számát.

3.7.5. Tétel. *Legyen T test, és $f \in T[x]$. Tegyük fel, hogy $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$, ahol $c, \alpha_1, \dots, \alpha_n \in T$ és $c \neq 0$ az f főegyütthatója. Ekkor*

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} c^{2n-1} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 .$$

Bizonyítás. A 3.7.2. Állítás miatt

$$R(f, f') = c^{n-1} f'(\alpha_1) \dots f'(\alpha_n) .$$

A 3.6.9. Gyakorlat szerint

$$f'(\alpha_i) = c(\alpha_i - \alpha_1)\dots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})\dots(\alpha_i - \alpha_n) .$$

Ezt az előző képletbe behelyettesítve, és az $\alpha_i - \alpha_j$ különbségek közül azokat megfordítva, ahol $i > j$, az állítást kapjuk. □

3.7.6. Definíció. Legyen T test, és az $f \in T[x]$ nem nulla polinom főegyütthatóját jelölje c. Ekkor a

$$\frac{(-1)^{\frac{n(n-1)}{2}} R(f, f')}{c}$$

kifejezést az *f diszkriminánsának* nevezzük.

Ha tehát f gyöktényezős alakja (akár egy bővebb testben) $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$, akkor diszkriminánsa a fenti tétel szerint

$$c^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 .$$

3.7.7. Következmény. *Ha T test, akkor egy T fölötti polinom diszkriminánsa akkor és csak akkor tűnik el, ha a polinomnak van többszörös gyöke egy alkalmas T-nél bővebb testben.*

Az $R(f, f')$ rezultánsnak vajon miért pont a $(-1)^{n(n-1)/2}/c$-szeresét választottuk f diszkriminánsának? A szakirodalom sem egységes ebben a tekintetben, a fenti választás mellett azonban több komoly érv szól. Egyrészt (az alábbi gyakorlat szerint) a másodfokú egyenlet esetében így vissza fogjuk kapni a megoldóképletbeli gyökjel alatti kifejezést, vagyis a diszkrimináns fogalma megegyezik a középiskolában megszokott szóhasználattal. Egy másik ok az, hogy a fenti szorzatformula szerint a diszkrimináns teljes négyzet (és így valós c és α_i esetén mindig nemnegatív), ennek jelentőségét az alább bizonyítandó állítás mutatja. Végül nagyon fontos szempont, hogy a széles körben használt matematikai számítógépes programok (`Maple, Mathematica, Mupad`) szintén a fenti definíciót használják.

3.7.8. Állítás. *Ha f valós együtthatós nem nulla polinom, akkor a diszkriminánsa akkor és csak akkor pozitív, ha minden komplex gyöke egyszeres, és a nem valós komplex gyökeinek száma néggyel osztható.*

Bizonyítás. Legyenek $\alpha_1, \dots \alpha_n$ az f komplex gyökei, feltehetjük, hogy mindegyik egyszeres (különben a diszkrimináns nulla lesz, és az állítás igaz). Kiszámítjuk a rezultáns előjelét a fenti szorzatképlet alapján. Nyilván $c^{2n-2} > 0$. A szorzat további tagjai az $i < j$ számpárokhoz tartozó $(\alpha_i - \alpha_j)^2$ tényezők. Mivel f valós együtthatós, minden gyökének a konjugáltja is gyök. Ha tehát $\overline{\alpha_i} = \alpha_k$ és $\overline{\alpha_j} = \alpha_\ell$, akkor a szorzatban szerepel az $(\alpha_k - \alpha_\ell)^2$ tényező is ($k > \ell$ esetén $(\alpha_\ell - \alpha_k)^2$ formában). Ha az $\{i, j\}$ és $\{k, \ell\}$ számpárok különbözők, akkor ez két különböző tényező, és szorzatuk pozitív valós (hiszen egy számot a konjugáltjával szoroztunk össze). Ha viszont $\{i, j\} = \{k, \ell\}$, akkor vagy $i = k$ és $j = \ell$, vagy $i = \ell$ és $j = k$. Az első esetben α_i és α_j valós számok, és $(\alpha_i - \alpha_j)^2$ pozitív valós. A második esetben α_i és α_j egymás konjugáltjai. Ekkor $\alpha_i - \alpha_j$ tisztán képzetes szám, és így a négyzete negatív valós. A konjugált nem valós gyökpárok mindegyike tehát egy negatív valós számmal járul hozzá a fenti szorzathoz. Így a szorzat akkor és csak akkor lesz pozitív, ha ezeknek a gyökpároknak a száma páros. □

3.7.1. Gyakorlat. Legyen $f(x) = ax^2 + bx + c$ másodfokú polinom. Mutassuk meg, hogy f diszkriminánsa $b^2 - 4ac$, vagyis a megoldóképletben a négyzetgyök alatt álló kifejezés. Az előző állítás alapján igazoljuk, hogy az f polinomnak akkor és csak akkor valósak a gyökei, ha a diszkriminánsa nemnegatív.

3.7.2. Gyakorlat. Legyen $f(x) = x^3 + px + q$. Mutassuk meg, hogy f diszkriminánsa $-27q^2 - 4p^3$, vagyis a Cardano-képletben a négyzetgyök alatt álló kifejezés -108-szorosa.

3.7.9. Példa. Oldjuk meg az alábbi egyenletrendszert a rezultáns felhasználásával.

$$\left.\begin{aligned} yx^2 + y^2 - 2 &= 0 \\ y^2x^2 + yx - 2 &= 0 \end{aligned}\right\}$$

A megoldás során mindkét egyenlet baloldalát x polinomjának képzeljük, és felírjuk a rezultánsukat. Az eredmény a következő lesz:

$$r(y) = \begin{vmatrix} y & 0 & y^2-2 & 0 \\ 0 & y & 0 & y^2-2 \\ y^2 & y & -2 & 0 \\ 0 & y^2 & y & -2 \end{vmatrix} = y^8 - 4y^6 + 5y^5 + 4y^4 - 10y^3 + 4y^2 \,.$$

A rezultáns akkor és csak akkor nulla, ha vagy mindkét főegyüttható nulla, vagy a két polinomnak van közös gyöke. A két főegyüttható y, illetve y^2. Mindkettő akkor és csak akkor nulla, ha $y = 0$. Az első egyenletből látszik, hogy erre az y-ra nincs megoldása az egyenletrendszernek. Tehát feltehetjük, hogy $y \neq 0$. Ebben az esetben az $r(y)$ polinom gyökei azok az y értékek, amelyekre az egyenletrendszer két egyenletének van (az x változóban) közös megoldása.

Normális körülmények között az $r(y)$ polinom gyökeit közelítő módszerekkel határoznánk meg. Most azonban szerencsénk van, mert ezt a polinomot viszonylag könnyű szorzattá alakítani. Az y^2 kiemelése után a racionális gyöktesszttel megállapíthatjuk, hogy a racionális gyökei 1 és -2. A megfelelő gyöktényezők kiemelése után $y^4-y^3-y^2+4y-2$ marad, ami kis ügyeskedéssel két másodfokú polinom szorzatára bontható:

$$r(y) = y^2(y-1)(y+2)(y^2-2y+2)(y^2+y-1)\,.$$

Ha például $y = 1$, akkor az egyenletrendszer első egyenlete $x^2 - 1 = 0$, a második $x^2+x-2=0$ lesz. Ezek közös gyöke csak az $x = 1$. Ugyanilyen számolással kapjuk meg az $r(y)$ többi gyökéhez is a megfelelő x értékeket. Végeredményben az egyenletrendszer összes megoldása a következő hat (x, y) pár lesz:

$$(1,\,1)\,,\quad (1,\,-2)\,,\quad (-1+i,\,1+i)\,,\quad (-1-i,\,1-i)\,,$$
$$\left(\frac{\sqrt{5}+1}{2},\,\frac{\sqrt{5}-1}{2}\right),\quad \left(\frac{1-\sqrt{5}}{2},\,\frac{-1-\sqrt{5}}{2}\right). \quad \square$$

A rezultáns tehát arra alkalmas, hogy két egyenletből egy olyan csináljon, amelyben már eggyel kevesebb ismeretlen van. Ha kettőnél több ismeretlenünk vagy egyenletünk van, akkor a módszert többször egymás után kell alkalmazni.

Gyakorlatok, feladatok

3.7.3. Gyakorlat. A rezultáns módszerével vezessük vissza az alábbi három egyenletrendszert egyismeretlenes egyenletre, és oldjuk is meg őket $\mathbb{C}$ fölött.

$$\begin{cases} (x-1)\cdot y^2+(x+1)\cdot y-2=0 \\ (x-1)\cdot y^2+\quad x\cdot y-1=0 \end{cases} \qquad \begin{cases} (x-1)\cdot y^2+(x+1)\cdot y-1=0 \\ (x-1)\cdot y^2+\quad x\cdot y-1=0 \end{cases}$$

$$\begin{cases} x^2 = y+z+1 \\ y^2 = z+x+1 \\ z^2 = x+y+1 \end{cases}$$

3.8. A harmad- és negyedfokú egyenlet

A harmadfokú egyenlet megoldási ötletéről és a Cardano-képletről már volt szó a komplex számok bevezetése kapcsán, de számos kérdés nyitva maradt. Azóta felépítettük azokat az eszközöket, amelyekkel a témát lezárhatjuk. A tárgyalás az előző szakaszhoz hasonlóan kissé vázlatos lesz, és csak arra az esetre szorítkozunk, amikor az egyenlet együtthatói komplex számok. Először röviden átismételjük, hogy meddig is jutottunk el az 1.2. Szakaszban.

Az általános harmadfokú egyenlet megoldásának kérdését visszavezettük arra az esetre, amikor az egyenlet

$$x^3 + px + q = 0$$

alakú. Megmutattuk, hogy ha u és v olyan számok, melyekre $uv = -p/3$ és $u^3+v^3 = -q$, akkor az $u + v$ szám biztosan megoldása az egyenletnek. Ezt az egyenletrendszert úgy próbáltuk megoldani, hogy az első egyenletet köbre emeltük. Ekkor az $s = u^3$ és $t = v^3$ értékekre

$$s = -\frac{q}{2} + \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \quad \text{és} \quad t = -\frac{q}{2} - \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

adódott. Ezekre az s és t számokra tehát $s + t = -q$ és $st = (-p/3)^3$ teljesül. Innen u-t és v-t köbgyökvonással akartuk meghatározni, és eredményül a Cardano-képletet kaptuk:

$$x = u + v = \sqrt[3]{s} + \sqrt[3]{t} = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\,.$$

Ezzel a képlettel több probléma is van. Nem mutattuk meg, hogy az egyenlet mindegyik megoldása megkapható ebből a képletből, és azt sem, hogy a képlet által adott szám megoldása az egyenletnek. Ennél súlyosabb probléma, hogy a képlet nem is egyértelmű, hiszen tudjuk, hogy egy nem nulla komplex számnak három különböző köbgyöke van. A képletet tehát elvileg $3 \cdot 3 = 9$-féle módon értékelhetjük ki.

Annyit azért tisztáztunk az 1.2.4 és az 1.2.10 gyakorlatok megoldása során, hogy a képletben (vagyis az s és t kifejezésekben) szereplő két négyzetgyököt úgy kell választani, hogy egymás ellentettjei legyenek. (Vigyázzunk, komplex számok esetén egy számnak két egyenrangú négyzetgyöke van, nincs közöttük kitüntetett, nem mondhatunk olyat, mint valósban, hogy a négyzetgyök mindig a nemnegatív értéket jelöli, lásd az 1.2.11. Gyakorlat megoldását). Ha ezt a két négyzetgyököt a képletben megcseréljük, akkor u és v kicserélődik.

3.8.1. Tétel. *Ha a Cardano-képletben szereplő u és v köbgyököket úgy választjuk, hogy szorzatuk $-p/3$ legyen, akkor a képlet az egyenlet megoldását szolgáltatja, és az egyenlet mindegyik megoldása megkapható ezen a módon.*

Bizonyítás. Bárhogyan is választjuk ki az u és v köbgyököket, $u^3 + v^3 = s + t = -q$ és $u^3v^3 = st = (-p/3)^3$ biztosan teljesülni fog. Ha $uv = -p/3$ is teljesül, akkor az imént felidézett állítás szerint $x = u + v$ tényleg megoldása az egyenletnek. Meg kell még mutatnunk, hogy az egyenlet mindegyik megoldása megkapható a képletből. Egyúttal gyakorlati útmutatót is adunk a képlet használatára.

Válasszuk külön azt az esetet, amikor $p = 0$. Ebben az esetben az egyenlet az $x^3+q = 0$ alakot ölti, megoldásai tehát a $-q$ szám köbgyökei, és ezért nem érdemes a képletet használni. Meg kell azonban mutatnunk, hogy a képlet ebben az esetben is kiadja az egyenlet megoldásait. Amikor behelyettesítünk, akkor a $(-q/2)^2$ számból kell négyzetgyököt vonni, ennek értékei $-q/2$ és $q/2$. Ha az s kifejezésben választjuk a $-q/2$, a t kifejezésben pedig a $q/2$ értéket, akkor $s = u^3 = -q$ és $t = v^3 = 0$ adódik. Így $v = 0$, és u a $-q$

szám valamelyik köbgyöke. Ezek szorzata tényleg $p/3 = 0$, és így a képlet tényleg kiadja az egyenlet megoldásait.

Tegyük most föl, hogy $p \neq 0$. Megmutatjuk, hogy u-nak szabad az s kifejezés *bármelyik* köbgyökét választani, a $v = -p/3u$ választás a t kifejezés egyik köbgyökét fogja eredményezni (és így az egyenletnek az egyik megoldását kapjuk). Tudjuk, hogy $st = (-p/3)^3$ (speciálisan s, és így u sem nulla). Ha tehát $u^3 = s$, akkor innen

$$v^3 = (-p/3u)^3 = (-p/3)^3/u^3 = st/s = t\,.$$

Tehát tényleg választhatjuk u-nak az s szám bármelyik köbgyökét.

Legyen az s három köbgyöke u_1, u_2, u_3, ekkor $v_i = -p/3u_i$ is kiadja a t szám három köbgyökét (hiszen három különböző számról van szó). Azt kell még megmutatni, hogy $u_i + v_i$ az egyenlet összes megoldása, azaz hogy

$$f(x) = x^3 + px + q = (x - u_1 - v_1)(x - u_2 - v_2)(x - u_3 - v_3)\,.$$

Ezzel valójában többet bizonyítunk: azt is megmutatjuk, hogy ha az f polinomnak vannak többszörös gyökei, akkor a Cardano-képletet az imént leírt módon használva minden gyököt annyiszor kapunk meg, amennyi a multiplicitása. A közvetlen beszorzás helyett rövidebb utat választunk.

Legyen $\alpha_i = u_i + v_i$, tudjuk, hogy ezek gyökei f-nek. Tegyük föl, hogy az α_i számok között van két különböző, mondjuk $\alpha_1 \neq \alpha_2$. Az f polinomban nem szerepel x^2-es tag, ezért gyökeinek összege nulla, és így harmadik gyöke csak $-\alpha_1 - \alpha_2$ lehet. Azt kell tehát belátni, hogy $-\alpha_1 - \alpha_2 = \alpha_3$. De ez igaz, mert egy komplex szám három köbgyökének az összege nulla, és így $u_1 + u_2 + u_3 = 0$, $v_1 + v_2 + v_3 = 0$, vagyis $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Ebben az esetben tehát készen vagyunk.

Ha az α_i számok mindhárman egyenlők, akkor, mivel összegük nulla, mindegyik nulla kell, hogy legyen. Így $u_i = -v_i = p/3u_i$, azaz $u_i^2 = p/3$. Ez lehetetlen, mert a $p/3$-nak csak két négyzetgyöke lehet, az u_1, u_2, u_3 pedig (a most vizsgált $p \neq 0$ esetben) páronként különböző. Ez az ellentmondás bizonyítja az állítást. (Az olvasó meggondolhatja, hogy a három α_i valójában csak a $p = q = 0$ esetben lehet egyenlő.) □

3.8.2. Tétel. *A komplex együtthatós $f(x) = x^3 + px + q$ polinomnak akkor és csak akkor van többszörös komplex gyöke, ha a Cardano-képletben a négyzetgyökjel alatt álló*

$$D = \left(-\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$$

kifejezés nulla. Ha a p és q együtthatók valósak, akkor $D \leq 0$ esetén mindegyik gyök valós, $D > 0$ esetén pedig egy valós gyök van, a másik két komplex gyök pedig egymás konjugáltja.

Bizonyítás. A 3.7.2. Feladatban kiszámoltuk, hogy az f polinom diszkriminánsa $-108D$. Ez akkor és csak akkor nulla, ha $D = 0$, ami az első állítást bizonyítja (hiszen a diszkrimináns akkor tűnik el, ha van többszörös gyök).

Tegyük fel, hogy p és q valós. Ha a polinomnak van nem valós gyöke, akkor ennek konjugáltja is gyök, a harmadik gyök pedig valós, ebben az esetben tehát három különböző gyök van. A nem valós gyökök száma 2, ami nem osztható néggyel, tehát a 3.7.8. Állítás szerint ilyenkor f diszkriminánsa, azaz $-108D$ negatív, tehát $D > 0$. A másik lehetőség az, ha három valós gyök van. Ekkor a nem valós gyökök száma nulla, ami néggyel osztható szám, és így a 3.7.8. Állítás szerint f diszkriminánsa, azaz $-108D$ nulla vagy pozitív, vagyis $D \leq 0$. □

Ez az eredmény megerősíti azt az anomáliát, amit konkrét példákon már megismertünk az 1.2. Szakaszban. Ha $D > 0$, akkor az egyetlen valós gyököt csak valósban számolva megadja a Cardano-képlet. Ha azonban három valós gyök van, akkor a Cardano-képletben negatív számból kell négyzetgyököt vonni, tehát ha komplex számokat nem használhatunk, akkor a képlet az egyenlet egyik gyökét sem adja meg! A régiek, akik még nem ismerték a komplex számokat, ezt *Casus irreducibilisnek,* megoldhatatlan esetnek nevezték.

A helyzet valójában még rosszabb: nemcsak a Cardano-képlettel, hanem *semmilyen más, a négy alapműveletet és valósban maradó akárhányadik gyökvonásokat tartalmazó, akármilyen bonyolult képlettel sem lehet általában kiszámítani a harmadfokú egyenlet gyökeit akkor, ha három valós gyök van.* Ez a tétel a Galois-elmélet eszközeivel bizonyítható. Magát a tételt nem bizonyítjuk, de egy testvérét később igen, nevezetesen azt, hogy az általános ötöd- (és magasabb) fokú egyenletet már komplex gyökvonások segítségével sem lehet általában megoldani, ezekre már nem létezik olyan megoldóképlet, amely az együtthatókból kiindulva a négy alapműveletet és az akárhányadik gyökvonásokat használja.

Természetesen mérnöki számításokhoz már a harmadfokú egyenletet sem a gyökképlettel érdemes megoldani, hanem közelítő módszerekkel. A közelítő módszerek azonban nem minden probléma megoldására alkalmasak. Ha például azt kell eldönteni, hogy van-e többszörös gyök, akkor a fenti elméletre, azaz a diszkrimináns vizsgálatára van szükség.

Ám egy olyan elméleti problémát, hogy létezik-e gyökképlet, nem a gyakorlati alkalmazások miatt érdemes vizsgálni. Mint a bevezetőben is írtuk, a matematikában általában nem lehet előre tudni, hogy mely kérdések a fontosak, mert ehhez nem vagyunk eléggé okosak! A jó problémák azok, amelyek új, még feltáratlan területekre, új jelenségek megértésére vezetnek. A keletkező elméletek azután már sokszor gyakorlati alkalmazásokat is adnak. Jó példa erre, hogy az egyenletek gyökképletének vizsgálata a Galois-elmélet kifejlődéséhez vezetett, ennek segítségével értettük meg a véges testek szerkezetét, ezeket pedig, szinte váratlan módon, alkalmazni lehet a híradástechnikában, azaz a kódelméletben. Minderről szó lesz később ebben a könyvben.

3.8.1. Gyakorlat. Mutassuk meg, hogy az $ax^2 + bx + c \in \mathbb{C}[x]$ polinom akkor és csak akkor négyzete egy $\mathbb{C}[x]$-beli polinomnak, ha $b^2 - 4ac = 0$ (itt $a = 0$ is megengedett).

3.8.3. Tétel. *Az általános negyedfokú komplex együtthatós polinomok gyökeit megkaphatjuk az együtthatókból a négy alapművelet és a gyökvonás segítségével.*

Bizonyítás. A negyedfokú egyenlet megoldóképlete annyira bonyolult, hogy nem szokás és érdemes felírni, hanem inkább egy módszert mutatunk a gyökök meghatározására. Csak a megoldás ötletének a bemutatására szorítkozunk, és a diszkussziót is elhagyjuk.

A főegyütthatóval leosztva az egyenlet a következő alakú lesz:

$$f(x) = x^4 + ax^3 + bx^2 + cx + d = 0\,.$$

A tervünk az, hogy f-et két másodfokú polinom szorzatára bontsuk, mert akkor már könnyű megkeresni a gyökeit. Ehhez egy harmadfokú egyenletet kell majd megoldanunk. A két másodfokú tényezőt $K+L$ és $K-L$ alakban keressük, az egyenletet tehát két négyzet különbségeként akarjuk felírni. A $K(x)$ polinomot

$$K(x) = x^2 + \frac{a}{2}x + u$$

alakban érdemes keresni (az x-es tag együtthatóját azért választjuk $a/2$-nek, hogy K^2-ben az x^3 együtthatója ugyanaz legyen, mint f-ben). Ekkor könnyű számolással adódik, hogy

$$f(x) = K(x)^2 - \left(\left(2u + \frac{a^2}{4} - b\right)x^2 + \left(au - c\right)x + \left(u^2 - d\right)\right)\,.$$

A zárójelben álló polinom akkor lesz egy $L(x)$ polinom négyzete, ha a diszkriminánsa nulla (3.8.1. Gyakorlat), azaz

$$(au - c)^2 - (8u + a^2 - 4b)(u^2 - d) = 0\,.$$

Ez u-ra harmadfokú egyenlet, amit az eredeti egyenlet *harmadfokú rezolvensének* nevezünk. Ezt u-ra megoldjuk, és így elvégezhetjük az f szorzatra bontását. □

Gyakorlatok, feladatok

3.8.2. Gyakorlat. Oldjuk meg az alábbi egyenleteket a komplex számok között.

(1) $x^3 - 6ix - i + 8 = 0$.
(2) $x^3 + 12x - 16i = 0$.
(3) $x^3 - 21x + 20 = 0$.
(4) $x^4 + x^2 + 4x - 3 = 0$.

3.8.3. Gyakorlat. Tekintsük a 3.3.10. Feladatban vizsgált $x^4 - 10x^2 + 1$ polinomot. Írjuk föl a harmadfokú rezolvensét, és keressük meg ennek mindhárom gyökét. Hogyan változik ennek a polinomnak a felbontása két másodfokú szorzatára, ha a rezolvensnek más-más gyökét használjuk?

3.8.4. Feladat. Mutassuk meg, hogy egy negyedfokú, racionális együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha sem neki, sem a harmadfokú rezolvensének nincs racionális gyöke.

3.8.5. Feladat. Legyen $f(x)$ páratlan fokú reciprok polinom (lásd 3.5.8. Feladat). Mutassuk meg, hogy f-nek gyöke a -1. Igazoljuk, hogy az $x^7 + 2x^6 - x^4 - x^3 + 2x + 1 = 0$ egyenlet megoldható gyökjelek segítségével (azaz visszavezethető legfeljebb negyedfokú egyenletre).

3.8.6. Feladat. Vezessük vissza az $x^8+2x^2+4x+2 = 0$ egyenletet negyedfokú egyenletre.

3.9. A körosztási polinom

Ebben a szakaszban speciális, konkrét polinomokról lesz szó: azokról, amelyeknek a gyökei pontosan az n-edik primitív egységgyökök. Ezek természetesen adódnak, amikor az $x^n - 1$ polinomot irreducibilisek szorzatára bontjuk $\mathbb{Z}$ fölött. Fel fogjuk őket használni a geometriai szerkeszthetőség elméletében is. Az alábbiak elolvasása előtt érdemes átismételni a komplex egységgyökökről és a rendjeikről tanult állításokat.

3.9.1. Definíció. Ha $n \geq 1$ egész, akkor Φ_n jelöli az *n-edik körosztási polinomot,* vagyis azt a normált polinomot, melynek gyökei pontosan a primitív n-edik egységgyökök (mindegyik egyszeres). Képletben:

$$\Phi_n(x) = (x - \xi_1) \dots (x - \xi_{\varphi(n)}) ,$$

ahol $\xi_1, \dots, \xi_{\varphi(n)}$ az összes primitív n-edik egységgyök, vagyis az összes n-edrendű komplex szám.

Látjuk, hogy Φ_n foka $\varphi(n)$. A definíciót kis n számok esetén közvetlenül felhasználhatjuk a körosztási polinomok kiszámítására. Nyilván

$$\Phi_1(x) = x - 1 \quad \text{és} \quad \Phi_2(x) = x - (-1) = x + 1 .$$

A negyedik egységgyökök (1, -1, i és $-i$) közül az i és a $-i$ negyedrendű, azaz primitív, és ezért

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1 .$$

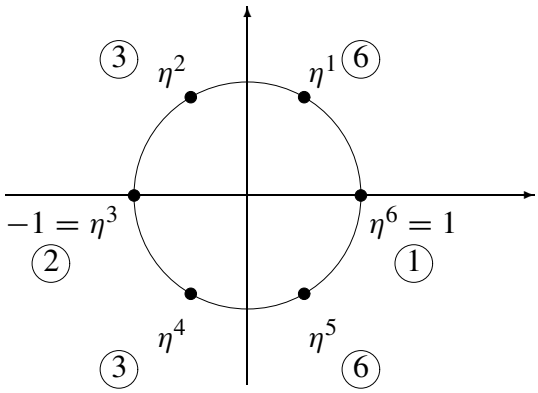
3.9.1. Gyakorlat. Mutassuk meg a megfelelő egységgyökök algebrai alakjának kiszámításával, hogy $\Phi_3(x) = x^2 + x + 1$, $\Phi_6(x) = x^2 - x + 1$ és $\Phi_{12}(x) = x^4 - x^2 + 1$.

Ez a közvetlen módszer általában nem működik: nagyobb n-ekre már a $\sin(2\pi/n)$ és $\cos(2\pi/n)$ értékét is csak közelítőleg tudjuk kiszámolni, a beszorzás pedig végképp elbonyolítja a dolgot. Pedig az eredmény szép: az összes eddig tárgyalt esetben egész együtthatós polinom jött ki, és látni fogjuk, hogy meglepő módon ez általában is így van.

Hogyan határozhatnánk meg például a Φ_3 polinomot? Ennek gyökei harmadik egységgyökök. A három harmadik egységgyök az $x^3 - 1$ polinom három gyöke. Ezek közül az 1 nem jó, mert az nem primitív harmadik egységgyök, de a másik kettő igen. Ezért ez a másik két szám az $(x^3 - 1)/(x - 1) = x^2 + x + 1$ polinomnak lesz gyöke. Azaz $\Phi_3(x) = x^2 + x + 1$.

3.9.2. Gyakorlat. Általánosítsuk ezt a gondolatmenetet a 3 helyett tetszőleges prímszámra.

Ha a hatodik körosztási polinomot akarjuk kiszámítani, akkor a hatodik egységgyököket kell áttekintenünk. Legyen $\eta = \cos 60^\circ + i \sin 60^\circ$. Ez primitív hatodik egységgyök, ezért a hatodik egységgyökök ennek a hatványai. A hatvány rendjére vonatkozó képletből látjuk, hogy $o(\eta) = o(\eta^5) = 6$ (ezek a hatodik primitív egységgyökök), $o(\eta^2) = o(\eta^4) = 3$ (tehát η^2 és η^4 pont a két primitív harmadik egységgyök), $o(\eta^3) = 2$ (valójában $\eta^3 = -1$), végül $o(\eta^6) = 1$ (és $\eta^6 = 1$). Az alábbi ábrán feltüntettük a hatodik egységgyököket, a bekarikázott számok pedig a rendjeik.



3.9.1. ábra. A hatodik egységgyökök rendjei.

Mivel $x^6 - 1$ gyökei pont a hat darab hatodik egységgyök, azt kapjuk, hogy

$$x^6 - 1 = (x - \eta)(x - \eta^2)(x - \eta^3)(x - \eta^4)(x - \eta^5)(x - \eta^6)\,.$$

Csoportosítsuk a gyöktényezőket az egységgyökök rendjei szerint.

$$\begin{array}{rccccc} x^6 - 1 = & \big[(x - \eta)(x - \eta^5)\big] & \big[(x - \eta^2)(x - \eta^4)\big] & (x - \eta^3) & (x - \eta^6) = \\ = & \Phi_6(x) & \cdot \quad \Phi_3(x) & \cdot \ \Phi_2(x) & \cdot \Phi_1(x)\,. \end{array}$$

Innen

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)}\,.$$

Mivel a Φ_1, Φ_2 és Φ_3 polinomokat már kiszámoltuk, osztással megkapjuk a keresett Φ_6-ot is. A számolást lerövidíti, ha felhasználjuk a korábban már bebizonyított $\Phi_1(x)\Phi_3(x) = x^3 - 1$ összefüggést:

$$\Phi_6(x) = \frac{x^6 - 1}{(x^3 - 1)\Phi_2(x)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1\,.$$

3.9.3. Gyakorlat. Kövessük végig ezt a gondolatmenetet $n = 6$ helyett $n = 12$-re, és határozzuk meg a Φ_{12} polinomot ezzel a módszerrel is.

Az elhangzott gondolatmenetet most már könnyű általánosítani.

3.9.2. Lemma. *Ha $n \geq 1$, akkor $\prod_{d|n} \Phi_d(x) = x^n - 1$.*

Bizonyítás. Legyen $\eta = \cos(2\pi/n) + i\sin(2\pi/n)$. Ekkor η primitív n-edik egységgyök, és ezért hatványai az n-edik egységgyököket adják meg. Ezek éppen az $x^n - 1$ gyökei, és mivel n különböző számról van szó, az $x^n - 1$ gyöktényezős alakja

$$x^n - 1 = (x - \eta)(x - \eta^2)\ldots(x - \eta^n)\,.$$

Ismét a megfelelő egységgyökök rendjei szerint csoportosítjuk a gyöktényezőket. Jelölje f_d a d rendű egységgyökökhöz tartozó gyöktényezők szorzatát. Így

$$x^n - 1 = \prod_d f_d(x)\,.$$

Elég belátni, hogy az itt fellépő d számok pontosan n osztói, és hogy ezekre $f_d = \Phi_d$.

Ha egy d szám fellép, vagyis ha $d = o(\eta^m)$ teljesül valamelyik m-re, akkor $(\eta^m)^n = (\eta^n)^m = 1^m = 1$ miatt n jó kitevője η^m-nek, és így $d \mid n$. Tehát a fellépő d számok tényleg csak n osztói lehetnek. Tegyük fel, hogy $d \mid n$. Ekkor Φ_d gyöktényezős felbontásában az *összes* d rendű komplex szám szerepel, f_d felbontásában pedig az olyan d rendű komplex számok szerepelnek, amik egyben n-edik egységgyökök is (mindegyik egyszer). De ezek ugyanazok a számok: mindegyik d-edik egységgyök egyben n-edik egységgyök is. Hiszen ha egy ξ számra $d = o(\xi) \mid n$, akkor $\xi^n = 1$, ezért ξ egy n-edik egységgyök. Beláttuk tehát, hogy $f_d = \Phi_d$. □

3.9.4. Gyakorlat. Igazoljuk, hogy tetszőleges $n \geq 1$ egészre $\sum_{d|n} \varphi(d) = n$.

3.9.3. Következmény. *Ha $n \geq 1$, akkor a Φ_n körosztási polinom egész együtthatós.*

Bizonyítás. Indirekt bizonyítunk, tegyük fel, hogy az állítás nem igaz, és legyen n a legkisebb olyan pozitív egész, melyre Φ_n nem egész együtthatós. Az előbbi lemma miatt

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d\neq n}} \Phi_d(x)}\,.$$

Az n minimalitása miatt a nevezőben csupa egész együtthatós polinom van, amik normáltak is. Ezért a nevező maga is normált, és egész együtthatós. Azt a gondolatot alkalmazzuk, amit már láttunk a 3.2.12. Gyakorlatban. Tudjuk, hogy minden olyan polinommal lehet maradékosan osztani, melynek a főegyütthatója invertálható. Ezért a számláló maradékosan eloszthatóa nevezővel $\mathbb{Z}[x]$-ben. A maradékos osztás ($\mathbb{C}$ fölötti) egyértelműsége miatt a hányados és a maradék ugyanaz, mint ha az osztást $\mathbb{C}$ fölött végeznénk. De $\mathbb{C}$ fölött tudjuk, hogy a hányados Φ_n és a maradék nulla. Tehát $\mathbb{Z}$ fölött is Φ_n a hányados, vagyis Φ_n mégis egész együtthatós. Ez az ellentmondás bizonyítja az állítást. □

Ebben a bizonyításban a teljes indukciónak egy formáját használtuk, feltettük, hogy az állítás minden n-nél kisebb értékre igaz, és beláttuk ebből, hogy n-re is igaz (ennek egy változatát a számelméletben végtelen leszállásnak is nevezik). Noha a fenti fogalmazásból is látszik, hadd hangsúlyozzuk még egyszer, hogy ilyenkor az indukciónak nincs „kezdő esete". Például az $n = 1$-et nem kell külön megnézni: a fenti gondolatmenetnek ekkor is működnie kell. Ha $n = 1$, akkor az, hogy minden n-nél kisebb értékre tudjuk az állítást, *üres feltétel.* A fenti képlet most így néz ki:

$$\Phi_1(x) = \frac{x^1 - 1}{\prod\limits_{\substack{d|1 \\ d\neq 1}} \Phi_d(x)}\,.$$

A nevező *üres szorzat* (ilyennel már találkoztunk a 2.2.23. Gyakorlatban), értéke tehát 1, és így a $\Phi_1(x) = x - 1$ összefüggést kapjuk, ami persze bizonyítja, hogy Φ_1 egész együtthatós.

A tanulság az, hogy miképpen egy programozónak figyelnie kell arra, hogy a programja akkor is jól működjön, ha mondjuk egy ciklus nullaszor fut le, *minden bizonyításban figyeljünk oda az „extrém" esetekre is, például arra, amikor egy halmaz, összeg, vagy szorzat üres, vagy valami nullával egyenlő, mert a bizonyításnak ilyenkor is működnie kell.*

Mint a Φ_6 példáján láttuk, az iménti bizonyítás egyben módot ad arra, hogy a körosztási polinomokat rekurzívan kiszámítsuk. A szakasz végén levő gyakorlatokban erre több példát is láthatunk. A 3.9.5. Gyakorlat, valamint a 3.9.9 és a 3.9.6. Feladatok lehetővé teszik, hogy az n-edik körosztási polinom kiszámítását visszavezessük arra az esetre, amikor az n páratlan, összetett, *négyzetmentes szám,* (vagyis minden prímosztója az első kitevőn szerepel).

A `Maple` program segítségével tetszőleges n esetén kiszámítható Φ_n (sőt, az eredményt a matematikai dokumentumok szedésére mindenki által használt, Donald Knuth által tervezett TEX nyelv formátumában is megkaphatjuk). Például a

```
with(numtheory):
for n from 3 by 2 to 105 do
  if issqrfree(n) and not isprime(n) then
    print(n, cyclotomic(n,x))
  fi
od;
```

parancssorozat kiírja páratlan, négyzetmentes, nem prím számokra a körosztási polinomokat 105-ig. Az eredmény az E. Függelékben olvasható. A listából megállapíthatjuk, hogy $n = 105$ a legkisebb olyan szám, melyre a Φ_n polinomnak van olyan együtthatója, ami nem a $0, 1, -1$ számok valamelyike. Ezt számítógép nélkül is megmutathatjuk, csak azt kell kiszámolni, hogy ha n két különböző páratlan prím szorzata, akkor Φ_n együtthatói csak a $0, 1, -1$ számok lehetnek.

Korábban azt állítottuk, hogy az $x^n - 1$ irreducibilis komponensei éppen a körosztási polinomok, más szóval, hogy a körosztási polinomok irreducibilisek $\mathbb{Z}$ fölött. Ezt most már be is tudjuk látni: a könyv első részének utolsó, és — véleményünk szerint — legszebb bizonyítása következik.

3.9.4. Tétel. *Mindegyik körosztási polinom irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ fölött.*

Bizonyítás. A 3.4.6. Tétel miatt a Φ_n körosztási polinom ugyanakkor irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ fölött, hiszen primitív (mert normált), és nem konstans. Bontsuk fel $\mathbb{Z}$ fölött irreducibilisek szorzatára: $\Phi_n(x) = f_1(x) \dots f_s(x)$. Az f_i tényezők főegyütthatója csak ± 1 lehet, tehát egyik sem konstans (hiszen akkor ± 1, vagyis egység lenne $\mathbb{Z}[x]$-ben), és így mindegyik f_i irreducibilis $\mathbb{Q}[x]$ fölött is. Azt kell megmutatnunk, hogy ebben a felbontásban csak egy tényező szerepel.

3.9.5. Lemma. *Legyen $p \nmid n$ prím. Ha egy ε számra $f_1(\varepsilon) = 0$, akkor $f_1(\varepsilon^p) = 0$.*

Ebből a lemmából könnyen következik a tétel. Valóban, mivel f_1 legalább elsőfokú, van egy $\varepsilon \in \mathbb{C}$ gyöke, ami persze Φ_n-nek is gyöke, azaz primitív n-edik egységgyök. Tehát az összes n-edik primitív egységgyök hatványa ε-nak, (1.5.8. Tétel) méghozzá (a hatvány rendjének képlete miatt) n-hez relatív prím kitevőjű hatványa. Tekintsük az ε^m számot, ahol $(m, n) = 1$. Az m szám felbontható prímek szorzatára: $m = p_1 \dots p_\ell$, ahol persze egyik p_j sem osztója n-nek. A lemma miatt ε^{p_1} gyöke f_1-nek. Most alkalmazzuk a lemmát az ε^{p_1} számra és a p_2 prímszámra. Azt kapjuk, hogy $(\varepsilon^{p_1})^{p_2} = \varepsilon^{p_1 p_2}$ is gyöke f_1-nek. A lemmát még $\ell - 2$-szer alkalmazva adódik, hogy $\varepsilon^{p_1 \cdots p_\ell} = \varepsilon^m$ is gyöke f_1-nek. Azaz f_1-nek gyöke az összes n-edik primitív egységgyök, és így Φ_n összes gyöktényezője már f_1-ben szerepel. Tehát f_1 a Φ_n felbontásának egyetlen tényezője. Így a 3.9.4. Tétel bizonyításához már csak a lemmát kell belátnunk, most ez következik.

Tegyük fel, hogy $f_1(\varepsilon) = 0$, de $f_1(\varepsilon^p) \neq 0$. Mivel $p \nmid n$, az ε^p is primitív n-edik egységgyök, azaz gyöke Φ_n-nek. Ezért ε^p gyöke valamelyik f_j polinomnak (ahol $j \neq 1$). Az indexek átszámozásával feltehetjük, hogy $j = 2$. Tehát $f_2(\varepsilon^p) = 0$.

Tekintsük az $f_1(x)$ és az $f_2(x^p)$ polinomok kitüntetett közös osztóját. Tudjuk, hogy ezt $\mathbb{Q}$ és $\mathbb{C}$ fölött kiszámítva ugyanazt a racionális együtthatós f polinomot kapjuk (3.2.3. Gyakorlat). Mivel a két polinomnak ε közös gyöke, az f polinom nem konstans (osztója $\mathbb{C}[x]$-ben $x - \varepsilon$). Ezért $f \mid f_1$-ből és f_1 irreducibilitásából az következik, hogy f az f_1 polinomnak asszociáltja, azaz nem nulla racionális konstansszorosa. Mivel $f(x) \mid f_2(x^p)$, ezért beláttuk, hogy $f_1(x)$ osztója az $f_2(x^p)$ polinomnak $\mathbb{Q}[x]$-ben. De akkor osztója $\mathbb{Z}[x]$-ben is, hiszen f_1 főegyütthatója ± 1, és így amikor a $g(x) = f_2(x^p)/f_1(x)$ osztást elvégezzük, akkor végig $\mathbb{Z}[x]$-ben maradunk (lásd 3.2.12. Gyakorlat, de hivatkozhatunk az első Gauss-lemma második következményére is.)

Vegyük a szereplő polinomok együtthatóit mod p, és jelölje felülvonás az így kapott polinomokat. Ekkor $\overline{f_1}(x)\overline{g}(x) = \overline{f_2}(x^p)$. A $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.8. Feladat), és ebben a feladatban azt is beláttuk, hogy $\overline{f_2}(x^p) = \overline{f_2}(x)^p$. Tehát $\overline{f_1} \mid \overline{f_2}^p$, ahol az oszthatóság $\mathbb{Z}_p[x]$-ben értendő. Mivel f_1 főegyütthatója ± 1, az $\overline{f_1}$ polinom sem konstans. Ez a polinom $\mathbb{Z}_p$ felett nem biztos, hogy irreducibilis, de mindenképpen van egy $\mathbb{Z}_p$ felett irreducibilis k osztója. Ekkor $k \mid \overline{f_1} \mid \overline{f_2}^p$, és mivel az irreducibilis polinomok $\mathbb{Z}_p[x]$-ben prímtulajdonságúak (hiszen $\mathbb{Z}_p$ test), azt kapjuk, hogy $k \mid \overline{f_2}$.

Találtunk tehát egy olyan $k \in \mathbb{Z}_p[x]$ nem konstans polinomot, ami $\overline{f_1}$-nak is és $\overline{f_2}$-nak is osztója. Ezért $k^2 \mid \overline{f_1 f_2}$. Viszont $f_1 f_2 \mid \Phi_n$, és $\Phi_n(x) \mid x^n - 1$. Ezért végülis $k^2 \mid \overline{x^n - 1}$. Ez azonban ellentmond a 3.6.7. Gyakorlat megoldásának, amely szerint $p \nmid n$ esetén az $x^n - 1$ polinomnak nincs többszörös tényezője mod p. Ezzel a lemma, és így a tétel bizonyítását is befejeztük. □

Gyakorlatok, feladatok

3.9.5. Gyakorlat. Számítsuk ki a prímhatvány-indexű körosztási polinomokat.

3.9.6. Feladat. Mutassuk meg, hogy ha $n > 1$ páratlan, akkor $\Phi_{2n}(x) = \Phi_n(-x)$.

3.9.7. Gyakorlat. Számítsuk ki az n-edik körosztási polinomot az összes $n \leq 20$ egészre.

3.9.8. Feladat. Bizonyítsuk be, hogy $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$, ahol μ az úgynevezett Möbius-függvény (B.0.9. Definíció).

3.9.9. Feladat. Legyenek $m \mid n$ pozitív egészek úgy, hogy n minden prímosztója osztja m-et is. Igazoljuk, hogy $\Phi_n(x) = \Phi_m(x^{n/m})$.

3.9.10. Gyakorlat. Számítsuk ki az előző feladat alapján a $\Phi_n(x)$ polinomokat abban az esetben, amikor $n = 36, 72, 144, 100$.

3.9.11. Feladat. Alkalmazzuk a gyökök és együtthatók összefüggését a 12-edik, 18-adik, illetve 24-edik primitív egységgyökök összegének és szorzatának kiszámítására. Általánosítsuk a feladatot n-edik primitív egységgyökökre.

3.9.12. Feladat. Határozzuk meg a Φ_n polinom együtthatóinak összegét.

3.9.13. Feladat. Határozzuk meg a $\Phi_n(-1)$ értékét.

3.9.14. Gyakorlat. Tegyük fel, hogy m és n relatív prímek. Mutassuk meg, hogy minden mn-edik primitív egységgyök egyértelműen előáll egy m-edik és egy n-edik primitív egységgyök szorzataként. Vezessük le ebből, hogy $\varphi(mn) = \varphi(m)\varphi(n)$.

3.9.15. Feladat. A 3.9.6. Feladat általánosításaként mutassuk meg, hogy ha m és n relatív prímek, akkor

$$\Phi_{mn}(x) = \prod_{o(\eta)=m} \Phi_n(\eta x)\,,$$

kivéve az $m = 2$, $n = 1$ esetben, amikor a két oldal egymás ellentettje.

3.9.16. Gyakorlat. Bontsuk az $x^{12} - 1$ polinomot irreducibilisek szorzatára $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$ és $\mathbb{Z}_5$ fölött.

3.9.17. Feladat. Legyen p prímszám, és $n = p^k m$, ahol már $p \nmid m$. Mutassuk meg, hogy modulo p a Φ_n egyenlő a $\Phi_m^{\varphi(p^k)}$ polinommal.

3.9.18. Gyakorlat. Mutassuk meg a 3.5.5. Feladat általánosításaként, hogy a prímhatvány-indexű körosztási polinomok alkalmas eltoltjára teljesül a Schönemann-Eisenstein kritérium feltétele.

3.9.19. Feladat. Igazoljuk, hogy a Φ_n polinom egy alkalmas eltoltjára akkor és csak akkor teljesül a Schönemann-Eisenstein, ha n prímhatvány, vagy egy páratlan prímhatvány kétszerese.

3.9.20. Gyakorlat. Határozzuk meg a `Maple` program segítségével azt a legkisebb n értéket, melyre a Φ_n polinomnak van kettőnél, illetve háromnál nagyobb abszolút értékű együtthatója.

3.10. Összefoglaló

Ebben a fejezetben a polinomok számelméletével, és ennek alkalmazásaival foglalkoztunk. Először tetszőleges szokásos gyűrűben vizsgáltuk a számelméleti alapfogalmakat. Ezek: oszthatóság, asszociált, egység, triviális felbontás, felbonthatatlan, prím, kitüntetett közös osztó és közös többszörös. Megfogalmaztuk a számelmélet alaptételének megfelelő állítást, az ezt teljesítő gyűrűket alaptételes gyűrűknek neveztük. Definiáltuk a kanonikus alak fogalmát, és ennek segítségével képletet adtunk az oszthatóságra, a kitüntetett közös osztóra és közös többszörösre.

Megmutattuk, hogy alaptételes gyűrűben igaz a kitüntetett közös osztó kiemelési tulajdonsága. Megfordítva, beláttuk, hogy ha egy szokásos gyűrűben teljesül, hogy bármely két f és g elem kitüntetett közös osztója létezik, és felírható $fr + gs$ alakban, akkor igaz a kitüntetett közös osztó kiemelési tulajdonsága, ezért minden irreducibilis elem prím, és innen következik már az alaptétel egyértelműségi állítása is. Mindez a 3.1. Szakaszban, illetve az azt követő feladatokban történt.

Általános tudásunkat polinomgyűrűkre alkalmaztuk. Megmutattuk, hogy egy szokásos gyűrű fölött minden olyan polinommal lehet, méghozzá egyértelműen, maradékosan osztani, amelynek a főegyütthatója invertálható; speciálisan test fölött minden nem nulla polinommal lehet (3.2.1. Tétel). A maradékos osztás segítségével test fölött elvégezhető a kitüntetett közös osztó kiszámítására szolgáló euklideszi algoritmus, és kétféleképpen is beláttuk, hogy ilyenkor tetszőleges f és g polinomok kitüntetett közös osztója felírható $fp + gq$ alakban (3.2.3. Tétel). Ebből test fölötti polinomgyűrűben levezettük a számelmélet alaptételét (az egyértelműség az előző bekezdésben írottakból következik, a létezés bizonyításához a fokszám tulajdonságait használtuk).

Bebizonyítottuk a számelmélet alaptételét $\mathbb{Z}[x]$-ben is (3.4.8. Tétel). Ennek az eredménynek a kulcsa a 3.4.6. Tétel, amelyben a $\mathbb{Z}$ fölötti irreducibilitást sikerült visszavezetni a $\mathbb{Q}$ fölötti irreducibilitásra: egy $f \in \mathbb{Z}[x]$ polinom akkor és csak akkor irreducibilis, ha vagy konstans prímszám, vagy $\mathbb{Q}$ fölött irreducibilis, és primitív (azaz nem emelhető ki belőle egységtől különböző egész szám). A bizonyításban szereplő nagyon hasznos technikai segédeszköz a két Gauss-Lemma: az első szerint a $\mathbb{Z}$-beli prímek $\mathbb{Z}[x]$-ben is prímek maradnak, vagy ami ezzel ekvivalens: primitív polinomok szorzata is primitív (3.4.3. Következmény); a második Gauss-Lemma pedig azt teszi lehetővé, hogy egy egész együtthatós polinom $\mathbb{Q}$ fölötti felbontását racionális konstansokkal való szorzás segítségével $\mathbb{Z}$ fölötti felbontássá módosíthassuk (3.4.5. Lemma). Észrevettük, hogy bizonyításunk nemcsak $\mathbb{Z}[x]$-ben, hanem tetszőleges alaptételes gyűrű fölötti polinomgyűrűben is működik, és így például $\mathbb{Z}[x_1, \ldots, x_n]$, és tetszőleges T testre $T[x_1, \ldots, x_n]$ is alaptételes.

Az alaptétel birtokában figyelmünk az irreducibilis polinomok felé fordult, az előző bekezdésben írottak miatt test fölöttiekre. Egy test fölötti polinom akkor és csak akkor irreducibilis, ha nem konstans, és nem bontható alacsonyabb fokú polinomok szorzatára. Egy polinomnak akkor és csak akkor van elsőfokú tényezője, ha van gyöke az adott testben

(3.3.3. Állítás). Ennek felhasználásával láttuk, hogy test fölött egy elsőfokú polinom mindig irreducibilis; egy másod- és harmadfokú akkor és csak akkor irreducibilis, ha nincs gyöke (3.3.4. Állítás); egy legalább negyedfokú polinom pedig nem lehet irreducibilis, ha van gyöke, de attól, hogy nincs gyöke, még nem biztos, hogy irreducibilis. Speciálisan $\mathbb{C}$ (illetve tetszőleges algebrailag zárt test) fölött az irreducibilis polinomok pontosan az elsőfokúak. A valós test fölött észrevettük, hogy egy polinom komplex gyökeinek konjugáltjai is ugyanannyiszoros gyökök (3.3.6. Lemma), ezért $\mathbb{R}$ fölött az elsőfokúakon kívül még azok a másodfokú polinomok irreducibilisek, amelyeknek nincs valós gyöke (és több irreducibilis polinom nincs). Következményként beláttuk, hogy páratlan fokú valós együtthatós polinomnak mindig van valós gyöke.

A racionális test fölött már nehezebb eldönteni az irreducibilitást. A gyökök meghatározása a racionális gyökteszt segítségével történhet (3.3.9. Tétel), így a legfeljebb harmadfokú polinomokkal nincs probléma. Ha szerencsénk van, használhatjuk az irreducibilitás eldöntésére a Schönemann-Eisenstein kritériumot (3.5.1. Tétel) a polinomra, vagy valamelyik eltoltjára. A polinomot felbonthatjuk $\mathbb{R}$ vagy $\mathbb{C}$ fölött, és ebből is következtethetünk néha arra, hogy irreducibilis-e $\mathbb{Q}$ fölött. Vizsgálhatjuk polinomunkat $\mathbb{Z}_p$ fölött alkalmas p prímszámra, ebben segít az az észrevétel, hogy itt tagonként lehet p-edik hatványra emelni (3.3.8. Feladat). Ezeket a módszereket a 107. oldal táblázatában foglaltuk össze.

Az n-edik körosztási polinom gyökei az n-edik primitív egységgyökök (3.9.1. Definíció), de ennek ellenére ez a polinom egész együtthatós, mert a 3.9.2. Lemma alapján rekurzívan is kiszámítható. A körosztási polinomok újabb példát szolgáltatnak a $\mathbb{Z}$ és a $\mathbb{Q}$ fölötti irreducibilitásra (3.9.4. Tétel).

Két polinom közös gyökei pontosan a kitüntetett közös osztójuknak a gyökei. Ez lehetővé teszi egy polinom többszörös gyökeinek meghatározását a formális deriválás módszerével (3.6.4. Tétel), mert egy k-szoros gyök a deriváltnak is legalább ($\mathbb{C}$ fölött pontosan) $k-1$-szeres gyöke. Így egy f polinom többszörös gyökei pontosan (f, f') gyökei lesznek. Azt, hogy két polinomnak van-e közös gyöke, a rezultáns módszerével is eldönthetjük (3.7.3. Tétel), ehhez egy speciális determinánst kell kiszámolni. A rezultáns segítségével egy többváltozós egyenletrendszert egyváltozós egyenletre vezethetünk vissza. Speciális esetként f és f' rezultánsának felírásával az f többszörös gyökeinek létezését is vizsgálhatjuk, így jutunk a diszkrimináns fogalmához (3.7.6. Definíció, 3.7.5. Tétel). A diszkrimináns előjele segít a konjugált komplex gyökpárok számának vizsgálatában is (3.7.8. Tétel).

Megmutattuk, hogy hogyan lehet a Cardano-képletből egy harmadfokú egyenlet összes gyökét megkapni (3.8.1. Tétel). Valós együtthatós egyenlet esetében a diszkrimináns akkor és csak akkor pozitív, ha az egyenletnek három valós gyöke van (3.8.2. Tétel). A diszkrimináns a négyzetgyökjel alatti kifejezés -108-szorosa, ezért amikor a gyökök mind valósak, akkor a Cardano-képletben negatív szám áll a négyzetgyökjel alatt, és így komplex számok használatára kényszerülünk. Szó esett arról, hogy három valós gyök esetén más módszerrel sem lehet olyan gyökképletet felírni, ami az egyenlet gyökeit komplex számok használata nélkül megadná (Casus irreducibilis). Végül röviden bemutattuk a negyedfokú egyenlet gyökjelekkel való megoldásának ötletét (3.8.3. Tétel).

A gyakorlatok és feladatok megoldásai

10. ÚTMUTATÁSOK, ÖTLETEK A FELADATOKHOZ

10.1. Komplex számok

1.1.4. Használjuk fel, hogy ha x és y egészek, akkor $x = mp + \overline{x}$ és $y = mq + \overline{y}$ alkalmas p, q egészekre, és helyettesítsük ezt be a bizonyítani kívánt képletekbe.

1.1.13. Teljes négyzetté alakítással vezessük vissza a feladatot négyzetgyökvonásra modulo 101. A 20 helyett a 121-ből vonjunk négyzetgyököt.

1.1.15. Színezzünk a modulo m maradékokkal. Vagdossunk le a sakktábláról olyan darabokat, ahol mindegyik maradékból ugyanannyi van. Ha r a k szám m-mel való osztási maradéka, akkor a bal felső $r \times r$-es négyzetben hány $r-1$ és hány 0 van?

1.1.16. Vizsgáljuk meg, hogy ezek a számok milyen maradékot adhatnak 3-mal osztva.

1.2.12. Mutassuk meg, hogy ha x nagy abszolút értékű szám, akkor $ax^3 + bx^2 + cx + d$ előjele ugyanaz, mint ax^3 előjele, mert az $|ax^3|$-höz képest a többi tag abszolút értékben még együttvéve is eltörpül.

1.3.7. Végezzük el a négyzetre emelést, és írjuk fel az eredmény valós, illetve képzetes részét. Így két egyenletet kapunk c-re és d-re.

1.4.8. A négyszöget a komplex számsíkra rajzolva képzeljük el, tehát a csúcsok komplex számok lesznek. Fejezzük ki a megfelelő négyzetek középpontjait a csúcsok segítségével. Használjuk fel, hogy két vektor akkor és csak akkor egyenlő hosszú és merőleges, ha az egyik a másiknak i-szerese.

1.4.9. A háromszög csúcsai segítségével fejezzük ki a szabályos háromszögek középpontjait. Használjuk fel, hogy egy háromszög akkor és csak akkor szabályos, ha az egyik oldalvektorát 60°-kal elforgatva egy másik oldalvektorát kapjuk. A $\cos 60^\circ + i \sin 60^\circ$ és a $\cos 120^\circ + i \sin 120^\circ$ számok közötti összefüggéseket ne az algebrai alakjukból, hanem a szabályos hatszög geometriai tulajdonságaiból vezessük le.

1.4.10. Mutassuk meg, hogy a $(z_3 - z_1)/(z_3 - z_2)$ szöge a $z_1z_2z_3$ háromszögnek a z_3-nál levő szöge. Használjuk a látókörről szóló geometriai tételt.

1.4.11. Használjuk fel az $(A - B)(C - D) + (A - D)(B - C) = (A - C)(B - D)$ azonosságot.

1.4.12. Az $\varepsilon = \cos(x/2) + i\sin(x/2)$ páros hatványait a mértani sor összegképletével adjuk össze. Az eredményt osszuk le ε egy olyan hatványával, hogy felhasználhassuk az $\varepsilon - (1/\varepsilon) = -2i\sin(x/2)$ és $\varepsilon^n - (1/\varepsilon)^n = -2i\sin(nx/2)$ összefüggéseket.

1.5.4. Melyik pontban lesz a bolha m lépés után? Hogyan írhatjuk fel oszthatóság segítségével, hogy ez a kiindulópont?

1.5.10. Keressük meg $-\varepsilon$ jó kitevőit.

1.5.14. Használjuk fel a binomiális tételt az $(1+1)^n$, $(1-1)^n$, $(1+i)^n$ összegekre.

1.5.15. Hatványozzuk a $\cos x + i\sin x$ számot a Moivre-képlet alapján is, és a binomiális tétel segítségével is.

10.2. Polinomok

2.2.1. Először az $\big((a*b)*(c*d)\big)*e = a*\Big(\big((b*c)*d\big)*e\Big)$ speciális esetet mutassuk meg. Az általános esetben is arra törekedjünk, hogy minden szorzatot olyan alakra hozzunk, mint a fenti azonosság jobb oldala, ahol az összes nyitózárójel „annyira balra van, amennyire csak lehet”. Alkalmazzunk teljes indukciót a szorzat hosszára nézve.

2.2.3. Mutassuk meg, hogy ha egy könyvespolcra a könyvek összevissza vannak feltéve, akkor rendet tudunk csinálni úgy, hogy mindig csak két szomszédos könyvet cserélünk ki.

2.2.5. Ha volna kettő, akkor számítsuk ki kétféleképpen a szorzatukat.

2.2.6.

(1) Tegyük fel, hogy v balinverze, és w jobbinverze u-nak. Számítsuk ki kétféleképpen a $v*u*w$ szorzatot.
(2) Ha u inverze u^{-1} és v inverze v^{-1}, akkor próbálkozzunk $v^{-1}*u^{-1}$-gyel.

2.2.7. Legyen a H részcsoport neutrális eleme f, és jelölje f^{-1} az f elemnek a G csoportbeli inverzét. Számítsuk ki kétféleképpen az $f*f*f^{-1}$ szorzatot.

2.2.9. A disztributivitást alkalmazzuk a $(0+0)r$ és az $r\big(s+(-s)\big)$ kifejezésekre.

2.2.10. Alkalmazzuk a 2.2.7. Feladat állítását.

2.2.13. Legyenek $u_1, \ldots, u_k$ a $\mathbb{Z}_m$-nek az m-hez relatív prím elemei, és u ezek egyike. Mutassuk meg, hogy $u *_m u_1, \ldots, u *_m u_k$ páronként különbözők.

2.2.18. Tudjuk, hogy $(\sqrt{2}-1)(\sqrt{2}+1) = 1$, tehát ezek invertálhatók. Hogyan lehetne ebből az összefüggésből további invertálható elemeket gyártani?

2.2.19. Vizsgáljuk meg, hogy egy nem nulla elem „abszolút értéke” lehet-e nulla.

2.2.21. Egy csoportban mely g elemekre igaz, hogy $g^2 = g$?

2.2.22. Tegyük fel, hogy van ilyen. Mutassuk meg, hogy az 1 képe szükségképpen 1 lesz, majd vizsgáljuk meg, hogy milyen tulajdonságú elem lehet az i képe.

2.4.8. Hány gyöke van az ax polinomnak?

2.4.9. Először olyan polinomot próbáljunk készíteni, amelynek gyöke az illető test mindegyik eleme.

2.4.11. Használjuk fel az interpolációról tanultakat. Egy binomiális együtthatót képzelhetünk-e polinomnak?

2.4.12. Mivel $f(14) = 440$, az f-et kereshetjük $(x - 14)g(x) + 440$ alakban, ahol g is egész együtthatós polinom.

2.4.13. Nem lehetséges. Bizonyítsunk az alappontok száma szerinti indukcióval, és használjuk a Newton-interpolációt.

2.4.14. Legyen $r \neq 0$ eleme R-nek. Mivel az interpoláció korlátlanul elvégezhető, van olyan $f \in R[x]$ polinom, melyre $f(0) = 0$ és $f(r) = 1$.

2.4.16. Álljon S azokból a függvényekből, melyeknek a 2 szám gyöke. A másik kérdésre a válasz: nem fordulhat elő. Ennek igazolásához használjuk föl, hogy nullosztómentes gyűrűben nem nulla elemmel szabad egyszerűsíteni (2.2.11. Gyakorlat).

2.5.2. Vizsgáljuk az elsőfokú polinomokat.

2.5.8. Emeljük négyzetre az $(x_1 + \cdots + x_n)$ összeget a 2.1.2. Gyakorlat felhasználásával.

2.5.10. A (4) állításhoz: helyezzük el a sokszöget úgy, hogy a csúcsai az n-edik egységgyökök legyenek, húzzuk meg az 1 csúcsból induló átlókat, ezek hosszainak szorzatát írjuk fel abszolút érték segítségével, majd használjuk fel a feladat (2) állítását.

2.6.5. Ha adott $k + 1$ darab különböző komplex szám n-es, akkor olyan n-határozatlanú polinomot keressünk, amelybe az első k darab szám n-est helyettesítve nullát kapunk, de a $k+1$-ediket helyettesítve nem. Minden $i \leq k$-ra keressünk egy olyan koordinátát, amelyben a $k + 1$-edik szám n-es különbözik az i-edik szám n-estől, és csak erre a koordinátára koncentráljunk.

2.7.9. Mutassuk meg, hogy $\sigma_1^{k_1} \dots \sigma_n^{k_n}$ homogén polinom, amely szükségképpen k-adfokú.

10.3. A polinomok számelmélete

3.1.18. Tegyük fel, hogy $p_1 \dots p_k = q_1 \dots q_\ell$ egy elem két felbontása irreducibilisek szorzatára. A p_1 prímtulajdonságát kihasználva keressük meg egy asszociáltját a q_j-k között, majd egyszerűsítsünk p_1-gyel.

3.1.21. Tudjuk, hogy $2 \mid 2 \cdot 2$. Osztója-e a 2 valamelyik tényezőnek a páros számok gyűrűjében is? Mutassuk meg, hogy $2 \cdot 18 = 6 \cdot 6$ a 36-nak két lényegesen különböző felbontása felbonthatatlanok szorzatára a páros számok gyűrűjében.

3.1.23. Használjuk fel, hogy $3 \cdot 3 = 9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

3.1.24. Az x^5y^2 és az x^2y^5 polinomoknak van-e kitüntetett közös osztójuk?

3.2.1. Ha $g = 0$, akkor nem oszthatunk vele maradékosan, hogyan végezzük ilyenkor az eljárást? Az is előfordulhat, hogy egyáltalán nincs nem nulla maradék az algoritmusban, mi ilyenkor a kitüntetett közös osztó?

3.2.4. Van I-ben legalacsonyabb fokú polinom?

3.2.6. Alkalmazzuk a 3.2.1, 3.1.16, 3.1.17, 3.1.18. Gyakorlatokat, illetve Feladatokat.

3.2.7. Tegyük fel, hogy van olyan nem konstans polinom, amely nem bontható fel irreducibilisek szorzatára. Legyen f a lehető legkisebb fokú ilyen polinom. Irreducibilis-e f?

3.2.17. Mutassuk meg, hogy minden ilyen I halmaz a legkisebb pozitív elemének a többszöröseiből áll. A 3.2.3. Tétel bizonyítását kövessük.

3.3.8. Használjuk fel a binomiális tételt. Illusztrációként érdemes elolvasni a 3.3.7. Gyakorlat megoldásának a középrészét is. A kis Fermat Tétel bizonyításához emeljük (tagonként) p-edik hatványra azt a b tagból álló $\mathbb{Z}_p$-beli összeget, amelynek mindegyik tagja 1.

3.3.10. Mutassuk meg a gyöktényezős alak beszorzásával, hogy x^4-10x^2+1 összes gyökei $\pm\sqrt{2} \pm \sqrt{3}$. A beszorzást végezzük el háromféleképpen is, mindig máshogy összepárosítva két-két gyöktényezőt. A $\mathbb{Q}$ feletti irreducibilitás bizonyításához a 3.3.10. Példában leírt módszert használjuk. Vizsgáljuk meg, hogy a $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ gyökvonások melyike végezhető el $\mathbb{Z}_5$, $\mathbb{Z}_7$, illetve $\mathbb{Z}_{11}$ fölött.

3.5.5. Használjuk fel, hogy $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.8. Feladat), valamint a következő összefüggést:

$$1 + x + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}\,.$$

3.5.8. Mutassuk meg, hogy $g(x) = x^n f(1/x)$.

3.5.12. Mutassuk meg, hogy $f\big(x + f(x)\big)$ osztható $f(x)$-szel.

3.5.13. Fogalmazzuk meg a Schönemann-Eisenstein kritériumot abban az esetben, amikor $\mathbb{Z}$ helyett a $\mathbb{C}[y]$ gyűrű feletti polinomokat vizsgáljuk. Megy-e a 3.5.2. Gyakorlatban leírt bizonyítás ebben az esetben is?

3.5.14. Tegyük föl, hogy $\sqrt[3]{4} = a + b\sqrt[3]{2}$. Mi lehet az $x^3 - 2$ és az $x^2 - ax - b$ polinomok kitüntetett közös osztója? Van-e közös gyökük?

3.6.6. Az $f/(f, f')$ polinomnak mik a gyökei, és hányszorosak?

3.6.8. Mutassuk meg, hogy ha f irreducibilis, akkor $(f,\ f')$ csak akkor lehet nem konstans, ha $f' = 0$. Milyen f polinomokra teljesül ez $\mathbb{Z}_2$ fölött? Használjuk fel, hogy $\mathbb{Z}_2$ fölött tagonként lehet négyzetre emelni (3.3.8. Feladat).

3.6.10. Ha $f'(b) = 0$, tudjuk-e módosítani f-et úgy, hogy b gyöke legyen?

3.6.11. Mutassuk meg, hogy ha c kivételes érték, akkor f'-nek és $f(x) - c$-nek van közös gyöke.

3.8.4. Mutassuk meg, hogy az $(x^2 + vx + w)(x^2 + sx + t)$ polinom harmadfokú rezolvensének $(w + t)/2$ gyöke lesz.

3.8.5. Legyen $z = x + (1/x)$. Az $x + 1$ gyöktényező kiemelése után kapott polinomot osszuk le x^3-nel, és ezt írjuk fel z (harmadfokú) polinomjaként.

3.8.6. Teljes négyzet-e $\mathbb{C}$ fölött a $-(2x^2 + 4x + 2)$ polinom?

3.9.6. Használjuk fel az 1.5.10. Feladat eredményét.

3.9.8. Legyen η primitív m-edik egységgyök, ahol $m \mid n$. Számítsuk ki, hogy a feladatbeli szorzatban az $x - \eta$ hányadik hatványon szerepel, majd alkalmazzuk a B.0.10. Állítást.

3.9.9. Használjuk fel az előző feladatot.

3.9.11. Alkalmazzuk a gyökök és együtthatók közötti összefüggéseket az n-edik körosztási polinomra. Mutassuk meg, hogy az n-edik primitív egységgyökök összege $\mu(n)$ (ahol μ a Möbius-függvény), szorzatuk pedig 1, kivéve $n = 2$-re, amikor -1.

3.9.12. Osszuk le a $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggést $x - 1$-gyel, és azután helyettesítsünk $x = 1$-et.

3.9.13. Számítsuk ki a $\Phi_n(-x)$ polinomot a 3.9.9. Feladat, illetve a 3.9.6. Gyakorlat segítségével (attól függően, hogy n osztható-e néggyel), majd használjuk fel az előző feladat eredményét.

3.9.15. Az előző gyakorlat szerint Φ_{nm}-et felírhatjuk az $x - \eta\varepsilon$ gyöktényezők szorzataként, ahol $o(\eta) = m$ és $o(\varepsilon) = n$. Csoportosítsuk ezeket a gyöktényezőket η szerint.

3.9.17. A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésből kiindulva, n szerinti indukcióval bizonyítsunk. Számoljunk eleve $\mathbb{Z}_p$ fölött. Használjuk fel a 3.9.4. Gyakorlatot és a 3.3.8. Feladatot (azaz a tagonkénti p-edik hatványozás lehetőségét).

3.9.19. Térjünk át $\mathbb{Z}_p[x]$-re, alkalmazzuk a 3.9.17. Feladatot, majd a 3.6.7. Gyakorlat megoldásának azt az állítását, hogy $p \nmid m$ esetén $x^m - 1$-nek nincs többszörös tényezője $\mathbb{Z}_p[x]$-ben.

11. MEGOLDÁSOK, EREDMÉNYEK

11.1. Komplex számok

1.1. Műveletek és tulajdonságaik.

1.1.3. Vagdossunk le olyan darabokat a sakktábláról, ahol minden ráírt számból ugyanannyi van. Ilyenek például a 8×1-es téglalapok, vagy a 8×8-as négyzetek. A vagdosást végezzük úgy, hogy a végén a bal felső sarokban álló 4×4-es négyzet maradjon meg (ez az ábrán is látható). Ebben 0 szerepel, de 7 nem. Tehát a nullák és hetesek száma eredetileg sem lehetett egyenlő.

1.1.4. Jelölje felülvonás a modulo m maradékképzést. Ahhoz, hogy ez a leképezés szorzattartó, azt kell igazolni, hogy $\overline{xy} = \overline{x} *_m \overline{y}$. A maradékképzés definíciója miatt $x = mp + \overline{x}$ és $y = mq + \overline{y}$, alkalmas p, q egészekre. Ezért

$$xy = (mp + \overline{x})(mq + \overline{y}) = m[mpq + p\overline{y} + \overline{x}q] + \overline{x}\ \overline{y}\,.$$

Tehát xy és $\overline{x}\ \overline{y}$ különbsége osztható m-mel, és ezért ez a két szám ugyanazt a maradékot adja m-mel osztva. De xy maradéka $\overline{xy}$, és $\overline{x}\ \overline{y}$ maradéka $\overline{x} *_m \overline{y}$ (a $*_m$ definíciója szerint). Tehát $\overline{xy} = \overline{x} *_m \overline{y}$.

Az összegtartás ugyanígy, de valamivel egyszerűbb számolással igazolható. Az 1.1.2-beli azonosságok igazolásához írjuk fel a megfelelő azonosságot egész számokra, majd vegyük mindkét oldal maradékát modulo m. Végül a kivonást definiáljuk az $x -_m y = x +_m (\overline{-y})$ képlettel (ellentett hozzáadása). A fenti módszerrel könnyű megmutatni, hogy $x -_m y = \overline{x - y}$, és hogy a felülvonás a kivonást is tartja.

1.1.5. Az osztás a szorzás inverz művelete, és így a $2 : 3$ (modulo 5 végzett) osztás eredménye akkor lesz x, ha $3 *_5 x = 2$. A táblázat 3-hoz tartozó sorában a 2 maradék a 4 oszlopában szerepel, tehát a $2 : 3$ osztás eredménye 4. Általában a $b : a$ osztás modulo 5 elvégzése azt jelenti, hogy az $a, b \in \mathbb{Z}_5$ maradékokhoz olyan $x \in \mathbb{Z}_5$ maradékot keresünk, melyre $a *_5 x = b$. Nullával nem tudunk osztani, hiszen ha $a = 0$, akkor $b \neq 0$ esetén nincs ilyen x, ha meg $b = 0$, akkor minden x jó, tehát az eredmény nem egyértelmű. Ugyanakkor modulo 5 minden nem nulla maradékkal tudunk osztani. Ez abból következik, hogy minden nullától különböző maradéknak van reciproka, mint az a táblázatból leolvasható: az 1-nek és 4-nek önmaga, a 2 és 3 pedig egymás reciprokai modulo 5. De a táblázatból közvetlenül is láthatjuk, hogy minden nem nulla maradékkal lehet osztani, hiszen minden nem nulla elem sorában minden maradék előfordul.

Modulo 6 az $1/3$ osztás sem végezhető el, hiszen $3 *_6 x$ csak 0 vagy 3 lehet, 1 soha. Könnyű meggondolni, hogy modulo 6 csak az 1 és 5 maradékokkal tudunk korlátlanul osztani, mert csak ezeknek van inverze (mindkettőnek önmaga).

1.1.6. A modulo 5 táblázatban teljesül a nullosztómentesség, mert a nulla a szorzástáblának csak az első sorában és az első oszlopában fordul elő. Modulo 6 viszont nem teljesül, mert például $2 *_6 3 = 0$.

1.1.7. Egyik sem helyes.

(1) Abból, hogy modulo 5 van megoldás, még nem következik, hogy az eredeti egyenletnek is van megoldása. (Az eredeti egyenletnek nyilván nincs megoldása, hiszen x^2 és y^2 mindenképpen nemnegatív egész számok, és így $x^2 + 10y^2 < 10$ csak úgy lehetne, ha $y = 0$, de a 6 nem négyzetszám.)

(2) Ez a gondolatmenet azonos az előzővel, tehát még mindig rossz. Az csak véletlen szerencse, hogy az egyenletnek most van megoldása, például $x = y = 1$, de igaz állításra is adható helytelen bizonyítás. (Például ugyanezzel a gondolatmenettel kijönne, hogy az $x^2 + 5y^2 = 16$ egyenletnek is van megoldása, ami nem igaz.)

1.1.8. Csak az $a = 0, 1, 2, 3, 4$ értékeket kell végignézni. Ha mondjuk 3^5 értékét akarjuk kiszámítani modulo 5, akkor a 3^5 szám $\mathbb{Z}$-ben való kiszámítása helyett gyorsabb eljárás az, ha eleve modulo 5 maradékokkal számolunk. A $*_5$ szorzást $*$-gal jelölve a 3 négyzete $3*3 = 4$, a 3 köbe tehát $3*3*3 = 3*4 = 2$, negyedik hatványa $3*2 = 1$, ötödik hatványa $3 * 1 = 3$. Láthatjuk, hogy a hatványok ebben az esetben periodikusan ismétlődnek, tehát nagyon nagy kitevőkre is gyorsan kiszámíthatnánk őket. Ezzel a módszerrel könnyű ellenőrizni az első oszthatóságot, és ugyanígy számolhatjuk ki azt is, hogy a második oszthatóság pontosan akkor teljesül, ha a nem osztható öttel. Az első állításra közvetlen bizonyítást is nyerhetünk, ha az $a^5 - a = a(a + 1)(a - 1)(a^2 + 1)$ szorzat alakot felhasználjuk.

1.1.9. A feladat eredménye:

(1) $6 \mid a^6 - a \iff$ az a szám nem $6k + 2$, sem nem $6k + 5$ alakú.
(2) $6 \mid a^5 - 1 \iff$ az a szám $6k + 1$ alakú.
(3) $6 \mid a^2 - 1 \iff$ az a szám $6k \pm 1$ alakú (azaz a relatív prím a 6-hoz).

1.1.10. Csak azt kell ellenőrizni, hogy 1, 3, 5, 7 modulo 8 vett négyzete 1. Sőt, elég a négyzetre emelést elvégezni a ± 1 és ± 3 számokra, hiszen 5 és -3, illetve 7 és -1 ugyanazt a maradékot adják 8-cal osztva. A közvetlen bizonyítás: ha a páratlan számot $2k + 1$ jelöli, akkor

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1 \,,$$

és itt a szomszédos k és $k + 1$ valamelyike páros, azaz $4k(k + 1)$ osztható 8-cal. Tanulságos, hogy ez utóbbi, némi ötletességet igénylő bizonyítást helyettesíthetjük az előbbi gondolatmenettel, ami a modulo 8 számolási apparátus birtokában teljesen mechanikusan felfedezhető.

1.1.11. Modulo 5 számolva azt kapjuk, hogy $3 *_5 \overline{y} = 2$. A táblázat 3-hoz tartozó sorából leolvashatjuk, hogy $\overline{y} = 4$ (valójában a $2 : 3$ osztást végeztük el). Tehát $y = 5k + 4$ alkalmas k egészre. Az eredeti egyenletbe visszahelyettesítve $x = -3k - 1$ adódik. Ez egész szám, tehát minden ilyen y-ra megoldást kaptunk. Így végtelen sok megoldás van, minden egész k-ra egy. Például $k = 0$ esetén $(x, y) = (-1, 4)$.

1.1.12. Az $x = 0, \ldots, 4$ értékeket végigpróbálva modulo 5 számolással azt kapjuk, hogy az első oszthatóság az $x = 5k + 3$ és $x = 5k + 4$ alakú számokra teljesül. A második oszthatóságot $x = 0, \ldots, 6$ helyettesítéssel modulo 7 vizsgálva kapjuk, hogy ez semmilyen x-re sem teljesül.

1.1.13. Itt már fárasztó volna a $0, \ldots, 100$ számokat mind behelyettesíteni. Helyette ki fogjuk használni, hogy a 101 *prímszám*, azaz ha osztója egy szorzatnak, akkor osztója valamelyik tényezőjének is. Ebből következik, hogy egy számnak legfeljebb két négyzetgyöke lehet modulo 101. Valóban, ha egy N számnak a is és b is négyzetgyöke modulo 101, akkor a^2 és b^2 ugyanazt a maradékot adja 101-gyel osztva, mint N. Ezért $101 \mid a^2 - b^2 = (a - b)(a + b)$, azaz $101 \mid a - b$, vagy $101 \mid a + b$. Az első esetben a és b egyenlők modulo 101, a másodikban ellentettek. Így az N számnak a-n kívül csak $-a$ lehet még négyzetgyöke modulo 101, más nem.

(1) Az oszthatóságot modulo 101 vizsgálva másodfokú egyenletet kapunk. Teljes négyzetté kiegészítéssel $x^2 - 2x + 2 = (x - 1)^2 + 1$. Legyen $y = x - 1$, ekkor $\overline{y}^2 = \overline{-1} = 100$. A 100-nak a 10 és a $\overline{-10} = 91$ négyzetgyöke, és a fentiek szerint több négyzetgyöke nincs modulo 101. Ezért $\overline{y} = 10$ vagy $\overline{y} = 91$. Tehát a megoldások: $x = 101k + 11$ és $x = 101k + 92$, ahol k egész.

(2) Most is az előző módszert akarjuk alkalmazni, de két lépés is nehézséget okoz. Az első a teljes négyzetté alakítás. Ehhez az x-es tag együtthatóját (ami most páratlan szám) el kellene tudni osztani kettővel. De ezt meg lehet tenni modulo 101, hiszen $13 = \overline{114}$, vagyis a feladatban 13 helyett 114-et írhatunk. Ekkor $x^2 - 114x - 3 = (x - 57)^2 - 3252$, és -3252 ugyanazt a maradékot adja 101-gyel osztva, mint -20. Tehát most az $(\overline{x} - 57)^2 = 20$ egyenletet kell megoldanunk. A második nehézség most következik: a 20-ból négyzetgyököt kell vonni modulo 101. Erre most nem tudunk más módszert, mint végigpróbálgatni a mod 101 maradékokat (amit el akartunk kerülni). Szerencsére azonban $20 = \overline{121}$, ami 11-nek a négyzete. Ezért a megoldások: $x = 101k + 46$ és $x = 101k + 68$.

A feladat tanulsága, hogy a másodfokú egyenlet „gyökképlete” valójában csak annyit tesz, hogy az egyenletet négyzetgyökvonásra vezeti vissza. Ezt a valós számok esetében kalkulátorral vagy táblázatosan közelítőleg el tudjuk végezni, és ezért érezzük úgy, hogy ez egy megoldóképlet.

1.1.14. Nem fedhető le. A bizonyítás lényegében ugyanaz, mint a 100×100-as tábla esetén, csak most a modulo 2 maradékokat írjuk a sakktáblára a „szokásos” szabály szerint,

és azt vesszük észre, hogy a két hiányzó mezőn ugyanaz a szám áll (tehát a maradékon különbözik a nullák és egyesek száma, márpedig ha létezne lefedés, akkor nem különbözne). Természetesen ezt a bizonyítást egyszerűbb úgy elmondani, hogy 0 és 1 felírása helyett a mezőket világosra és sötétre festjük, ahogy az a sakktáblán amúgy is szokásos.

1.1.15. Ha $m \mid k$, akkor a lefedés nyilván (például soronként) lehetséges. Ha nem, akkor számozzuk meg a sakktábla mezőit a szokásos módon a modulo m maradékokkal. Ha lenne jó lefedés, akkor most is az derülne ki, hogy a $0, 1, \ldots, m-1$ mindegyikét ugyanannyiszor írtuk fel a sakktáblára. Az 1.1.3. Gyakorlat megoldásában szereplő vagdosási eljárással azt kapjuk, hogy ha r az k szám m-mel való osztási maradéka, akkor a bal felső $r \times r$-es négyzetben is ugyanannyiszor szerepel a $0, 1, \ldots, m-1$ számok mindegyike. Az $r-1$-es szám ennek a kis négyzetnek minden sorában pont egyszer szerepel (a mellékátló áll csupa $r-1$-ekből), azaz összesen r-szer. Tehát mind az m szám ennyiszer kell, hogy szerepeljen, azaz $mr = r^2$, hiszen ebben a négyzetben összesen r^2 szám van. Ez ellentmondás, mert $r < m$. (Máshogy is befejezhetjük a bizonyítást, ha észrevesszük, hogy a 0 az $r \times r$-es négyzet mindegyik sorában legfeljebb egyszer szerepelhet, de a második sorban egyáltalán nincs 0, és így ebben a négyzetben legfeljebb $r-1$ darab 0 lehet.)

1.1.16. Vizsgáljuk p-t modulo 3. Ha a maradék 1 vagy 2, akkor p^2+2 maradéka 0, azaz $3 \mid p^2+2$. Mivel feltettük, hogy p^2+2 is prímszám, ez csak úgy lehet, ha $p^2+2 = \pm 3$, azaz $p^2 = 1$, vagy $p^2 = -5$, de mindkettő lehetetlen (hiszen ± 1 nem prím). Tehát a p maradéka hárommal osztva csak 0 lehet, és mivel p prím, azt kapjuk, hogy p más, mint ± 3, nem lehet. Ebben az esetben viszont p^3+4 vagy 31, vagy -23, és mindkettő tényleg prímszám.

Ha azt tesszük fel, hogy p is és p^2+5 is prímszám, akkor a fenti gondolatmenetből most is látszik, hogy p csak ± 3 lehet. De ekkor $p^2+5 = 14$, ami nem prím. Tehát nincs ilyen p, és így a második állítás is igaz! Hiszen az összes ilyen prímre teljesül, hogy p^3+4 is prímszám (mert nincs egy sem)! Senki sem vonja kétségbe, hogy e könyv minden olvasója halandó, még akkor sem, ha történetesen senki sem olvassa el a könyvet. Sőt, az is igaz állítás, hogy ha p és p^2+5 is prímszám, akkor $2 \cdot 2 = 5$, hiszen hamis feltételből bármi következik.

Mindebből látszik, hogy az első megoldásban, amikor már kijött, hogy $p = \pm 3$, *nem kell ellenőrizni, hogy* p^2+2 *ilyenkor prímszám-e.* Ha nem lenne az, attól még az állítás érvényben maradna, legfeljebb csak még kevesebb p tenne eleget a feltételeknek.

1.2. A harmadfokú egyenlet megoldásának problémája.

1.2.1. Az x helyébe $y+w$-t írva $y^2+(2w+p)y+(w^2+pw+q) = 0$ adódik. Akkor tudjuk ezt közvetlenül, egy négyzetgyökvonással megoldani, ha nincs az egyenletben y-os tag, azaz ha $2w+p = 0$, vagyis $w = -p/2$. Ilyenkor $y^2 = p^2/4 - q$, ahonnan y, majd $x = y - p/2$ is kifejezhető, és a másodfokú egyenlet szokásos gyökképletét kapjuk.

1.2.2. Az x helyébe $y+w$-t írva, és az $(y+w)^3 = y^3+3y^2w+3yw^2+w^3$ azonosságot használva azt kapjuk, hogy az x^2-es tag együtthatója $3aw+b$. Ez pontosan akkor lesz nulla, ha $w=-b/3a$. A helyettesítést elvégezve $p=3aw^2+2bw+c$ és $q=aw^3+bw^2+cw+d$ adódik. (Azaz q az eredeti egyenlet baloldalának a w helyen felvett értéke).

1.2.3. Nem láttuk be még azt sem, hogy az egyenletnek *van* ilyen gyöke. Azt mutattuk meg, hogy *ha* az x ilyen alakú, *akkor* megoldása az egyenletnek. Egyelőre csak reménykedünk, hogy a gyököket mind megkapjuk majd ezzel az eljárással.

A következő példa érzékelteti, hogy ezt az állítást nem láttuk be. Képzeljük el, hogy az $x^3+x+1=0$ egyenletet modulo 3 akarjuk megoldani. Mivel modulo 3 a szokásos szabályokkal számolhatunk, sőt a nem nulla maradékokkal könnyen láthatóan még osztani is lehet modulo 3, az $x^3+px+q=0$ megoldásához levezetett képletek modulo 3 is érvényesek. Az egyenletnek nyilván gyöke az 1 modulo 3. De $-3uv=p=1$ soha nem teljesülhet, hiszen a baloldal mindenképpen nulla lesz modulo 3.

1.2.4. Ha x és y megoldása az egyenletrendszernek, akkor az első egyenletből $y=a-x$, ezért $x(a-x)=b$, azaz $x^2-ax+b=0$, tehát x megoldása a $z^2-az+b=0$ másodfokú egyenletnek. Hasonló számolással (vagy annak kihasználásával, hogy az egyenletrendszer szimmetrikus x-ben és y-ban) látjuk, hogy y is megoldása ennek a másodfokú egyenletnek.

Megfordítva, ha u megoldása a $z^2-az+b=0$ egyenletnek, akkor $u^2-au+b=0$, így

$$z^2-az+b = z^2-az+b-(u^2-au+b) = (z-u)(z-(a-u))\,.$$

Két valós szám szorzata csak akkor lehet nulla, ha valamelyik tényező nulla. Tehát a $z^2-az+b=0$ egyenlet megoldásai u és $a-u$, és más megoldása nincs. Mivel $u+(a-u)=a$ és $u(a-u)=au-u^2=b$, ezért tényleg az egyenletrendszer megoldását kaptuk.

Összefoglalva tehát a következő állítást láttuk be. A $z^2-az+b=0$ egyenletnek legfeljebb két valós megoldása van.

- Ha kettő van: $u_1\neq u_2$, akkor az egyenletrendszernek is két megoldása van (és több nincs): $(x,\,y)=(u_1,u_2)$ és $(x,\,y)=(u_2,u_1)$.
- Ha csak egy van, és ez u (ilyenkor tehát $z^2-az+b=(x-u)^2$ teljesül), akkor az egyenletrendszernek is egy megoldása van (és több nincs): $(x,\,y)=(u,u)$.
- Ha egy sincs, akkor az egyenletrendszernek sincs megoldása.

1.2.6. Ha az x-es tagot akarjuk eltüntetni, akkor olyan w-t kell választanunk, melyre $3aw^2+2bw+c=0$. Ez másodfokú egyenlet w-re, aminek nem is biztos, hogy van valós megoldása, és ha van is, a kapott négyzetgyökös kifejezéssel nehezebb számolni, mint amikor az x^2-es tagot tüntetjük el.

Ha viszont a konstans tagot akarjuk eltüntetni, akkor olyan w-t kell keresni, melyre $aw^3+bw^2+cw+d=0$. Vagyis w megoldása kell, hogy legyen az eredeti egyenletnek! Tehát ezt a helyettesítést már csak akkor tudjuk elvégezni, ha ismerünk egy megoldást, márpedig a cél éppen a megoldások megkeresése lenne. Ezért hangsúlyoztuk azt, hogy

az x^2-es tag kiejtéséhez használt w (és az új egyenletben keletkező p és q) konkrétan kifejezhető az eredeti egyenlet együtthatóiból.

1.2.7. Ez a gondolatmenet az 1.2.4. Gyakorlat fenti megoldásnak csak az első bekezdését pótolja.

1.2.8. Legyen $u = \sqrt[3]{7+\sqrt{50}}$ és $v = \sqrt[3]{7-\sqrt{50}}$, továbbá $x = u + v$. Mint láttuk, $x^3 = u^3 + v^3 + 3uv(u+v)$. Mivel

$$u^3 + v^3 = (7+\sqrt{50}) + (7-\sqrt{50}) = 14$$

és

$$uv = \sqrt[3]{(7+\sqrt{50})(7-\sqrt{50})} = \sqrt[3]{-1} = -1\,,$$

ezért azt kapjuk, hogy $x^3 = 14 + 3\cdot(-1)\cdot(u+v) = 14 - 3x$. Mivel x egész szám, osztója kell legyen a 14-nek. A ±1, ±2, ±7, ±14 értékeket kipróbálva azt kapjuk, hogy csak $x = 2$ teljesíti az $x^3 = 14 - 3x$ összefüggést. Ezzel azt láttuk be, hogy *ha* a kifejezés értéke egész szám, *akkor* csak 2 lehet, de még nem tudjuk, hogy x tényleg egész szám-e.

A $0 = x^3 - 14 + 3x = (x-2)(x^2+2x+7)$ szorzat alakból az adódik, hogy vagy $x = 2$, vagy $x^2 + 2x + 7 = 0$. Ez utóbbi összefüggést semmilyen valós x szám nem teljesíti, ezért beláttuk, hogy a feladatbeli kifejezés értéke 2.

Másik megoldásként vegyük észre, hogy $7+\sqrt{50} = (1+\sqrt{2})^3$ és $7-\sqrt{50} = (1-\sqrt{2})^3$, ahonnan ismét $x = 2$ adódik.

1.2.9. Az első állításhoz azt kell belátni, hogy $1+\sqrt{-1}$ negyedik hatványa -4. Ez közvetlen számolással látható, akár azonnal negyedik hatványra emelve a kifejezést, akár azt észrevéve, hogy $(1+\sqrt{-1})^2 = 2\sqrt{-1}$. Hasonlóan kapjuk, hogy az

$$1-\sqrt{-1}, \qquad -1+\sqrt{-1}, \qquad -1-\sqrt{-1}$$

kifejezések negyedik hatványa is -4. Később majd bebizonyítjuk, hogy ezeken kívül más hasonló kifejezés nincs, aminek a negyedik hatványa -4 lenne.

1.2.10. A felsorolt négy esetből kettőben ugyanaz a szám jön ki (csak felcserélődik u és v), a másik két esetben azonban általában nem is kapunk megoldást (mert a képlet eredménye nem $u+v$ lesz, hanem $2u$, illetve $2v$). Vigyázzunk, u^3 és v^3 a $z^2 + qz - (p/3)^3$ másodfokú egyenlet mindkét gyökét ki kell, hogy adja (lásd az 1.2.4. Gyakorlat megoldását), és ezért nem választhatjuk a négyzetgyök előjelét mindkétszer ugyanannak. A képlet mindazonáltal helyesen van felírva, mert valós számok körében az a megállapodás, hogy a négyzetgyök, ha elvégezhető, mindig a pozitív eredményt jelöli.

1.2.11. Nem, hanem csak azt jelenti, hogy nagyon gondosan meg kell vizsgálnunk, hogy az új kifejezésekkel milyen szabályok szerint számolhatunk. Ez az átalakítás mindössze azt mutatja, hogy a $\sqrt{ab} = \sqrt{a}\sqrt{b}$ összefüggés (amit felhasználtunk) nem fog érvényben maradni az új kifejezésekre.

1.2.12. A részletes megoldás (harmadfokú helyett tetszőleges páratlan fokú polinomra) elolvasható az A.0.4. Tétel bizonyításában.

1.3. Számolás komplex számokkal.

1.3.1. Ha lehetne, azaz egyenlők lennének, akkor a $2 + 3i = 4 + 5i$ egyenlőségből átrendezéssel $2i = -2$ adódna, négyzetre emelve $-4 = 4$, ami ellentmondás. Ez mutatja, hogy általában az $a + bi$ és $c + di$ számokat különbözőnek kell definiálnunk, ha $a \neq b$ vagy $c \neq d$. Ha így teszünk, akkor még reménykedhetünk, hogy a komplex számokkal való számolás nem vezet majd ellentmondásra.

1.3.2. Legyen $x = a + bi$, $y = c + di$ és $z = e + fi$. Ekkor az összeadás és a szorzás definícióját alkalmazva

$$(x + y)z = ((a + c) + (b + d)i)(e + fi) = \\ = (ae + ce - bf - df) + (af + cf + be + de)i \, .$$

Az $xz + yz$ kifejezést hasonlóan kiszámítva ugyanezt a végeredményt kapjuk.

1.3.3. A z számot $a + bi$ alakban kereshetjük. Ekkor

$$1 = (a + bi)(1 + i) = (a - b) + (a + b)i \, .$$

Két komplex szám akkor egyenlő, ha a valós és a képzetes részeik is egyenlők. A valós részek az $1 = a - b$, a képzetes részek a $0 = a + b$ egyenlőséget adják. Az egyenletrendszert megoldva $z = (1/2) - (1/2)i$ adódik.

1.3.4. Ha z valós, akkor $z\overline{z} = z^2$. Ezért pozitív z esetén $z\overline{z}$ négyzetgyöke maga z lesz. Ha viszont z negatív valós szám, akkor $z\overline{z}$ négyzetgyöke $-z$ lesz, hiszen valós szám esetében a négyzetgyökjel a négyzetgyök két értéke közül mindig a nemnegatívat jelöli.

1.3.5.

(1) Az eredmények $5 + i$, $-i$, $(1/13) + (5/13)i$.
(2) Mindkét eredmény 1. Az első tört esetében ez még kiszámolható, a második esetében már nem igazán. Azt kell észrevenni, hogy a számláló és a nevező abszolút értéke ugyanaz, és az 1.3.10. Gyakorlat szerint az abszolút érték tartja az osztást.
(3) $(1+i)^2 = 2i$, ezért $(1+i)^4 = (2i)^2 = -4$. Mivel $1241 = 4 \cdot 310 + 1$, az eredmény $(1 + i)^{1241} = (-4)^{310}(1 + i) = 2^{620} + 2^{620}i$.

1.3.6.

(1) $0 = x^2 + 1 = (x + i)(x - i)$, tehát a nullosztómentesség miatt $x = i$ vagy $x = -i$.
(2) $x^2 + 12 = (x + 2\sqrt{3}i)(x - 2\sqrt{3}i)$, ezért $x = \pm 2\sqrt{3}i$.
(3) $0 = x^2 + 2x + 2 = (x + 1)^2 + 1$ (a másodfokú egyenlet megoldási módszerét alkalmaztuk). Innen (1) szerint $x + 1 = \pm i$, tehát $x = -1 \pm i$.
(4) $0 = x^2 + 2ix - 1 = (x + i)^2$, tehát $x = -i$.

1.3.7. Ha $-21+20i=(c+di)^2=c^2-d^2+2cdi$, akkor a valós és képzetes rész egyértelműsége miatt $c^2-d^2=-21$ és $cd=10$. Tehát $c=10/d$, és a másik egyenletbe visszahelyettesítve, majd d^2-tel szorozva d^4-21d^2-100 adódik. Ez d^2-re másodfokú egyenlet, a megoldóképletből $d^2=25$ vagy $d^2=-4$. Ez utóbbi lehetetlen, mert d valós. Tehát $d=\pm5$, és akkor $c=10/d$ miatt $c+di=\pm(2+5i)$.

Ez a gondolatmenet elmondható a $-21+20i$ helyett az általános $a+bi$-re is. A számolást elvégezve $d^2=(-a\pm\sqrt{a^2+b^2})/2$ adódik. Amikor a négyzetgyök előtt negatív előjel van, akkor biztosan negatív eredményt kapunk d^2-re, mert $\sqrt{a^2+b^2}\geq|a|$, ez tehát hamis gyök. Amikor a négyzetgyök előtt pozitív előjel van, akkor ugyanezért d^2-re nemnegatív eredményt kapunk. A $2cd=b$ összefüggés alapján c értékét is megkaphatjuk. A nevezőbeli csúnya gyökös kifejezéstől megszabadulhatunk, ha a törtet $\sqrt{a+\sqrt{a^2+b^2}}$-tel bővítjük. De azt is megtehetjük, hogy inkább c értékét is a d-hez hasonlóan, a megfelelő másodfokú egyenletből kapjuk meg. Bármelyik módszerrel számolunk, a végeredmény a következő lesz:

$$\sqrt{a+bi}=\pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}\pm i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}\,.$$

Ez látszólag négy megoldás, ezért hozzá kell tenni, hogy a $2cd=b$ összefüggés miatt pozitív b esetén a két négyzetgyök előjelét egyformának, negatív b esetén különbözőnek kell választani. A képletből látszik, hogy *minden nem nulla komplex számnak pontosan két négyzetgyöke van a komplex számok között.* Ezt a következő pontban más módszerrel is be fogjuk látni. A most levezetett képletet nem érdemes megtanulni, inkább a levezetéséhez használt módszert (vagy a következő pontban tanulandókat) érdemes alkalmazni, ha négyzetgyököt kell vonni.

Az $x^2+(i-2)x+(6-6i)=0$ egyenlet megoldásához vegyük észre, hogy **a másodfokú egyenlet megoldásakor használt módszerünk komplex számokra is ugyanúgy érvényes.** Valóban, ellenőrizhetjük, hogy az 1.2.1. Kérdés megoldásakor csak a „szokásos" számolási szabályokat használtuk (amik az 1.3.2. Állításban vannak felsorolva), valamint azt, hogy a komplex számok között is lehet osztani. Tehát a fenti egyenlet megoldásához egyszerűen behelyettesíthetünk a gyökképletbe. A négyzetgyök alatt pontosan $-21+20i$ fog állni, amiből most vontunk négyzetgyököt. Az eredmény $2+2i$ és $-3i$.

1.3.8. Az első négy egyenlet mindegyikére alkalmazhatjuk a másodfokú egyenlet megoldóképletét, és az előző feladatban leírt négyzetgyökvonási eljárást.

(1) $(1\pm i)/\sqrt{2}$.
(2) $(-3\pm\sqrt{7}i)/2$.
(3) $3-i$ és $-1+2i$.
(4) $1-i$ és $(4-2i)/5$.
(5) Vegyük mindkét oldal abszolút értékét. Mivel $|x|=|\overline{x}|$, de $|3+2i|\neq1$, csak az $x=0$ megoldás. Második (csúnyább, de mechanikus) megoldás: az $x=a+bi$

helyettesítéssel, a szorzást elvégezve

$$a + bi = (3a + 2b) + (2a - 3b)i$$

adódik. A valós részeket nézve innen $a = 3a + 2b$, a képzetes részeket nézve $b = 2a - 3b$. Ennek az egyenletrendszernek csak $a = b = 0$ megoldása.

(6) Írjuk x-et $a + bi$ alakba. Ekkor $a + bi = 2a$ adódik, tehát $a = 2a$ és $b = 0$. Vagyis csak az $x = 0$ nulla megoldás. Eljárhattunk volna úgy is, hogy észrevesszük: x csak valós lehet, mert az egyenlet jobboldala valós, de valós szám valós része önmaga, tehát az $x = 2x$ egyenletet kell megoldanunk.

1.3.9. Legyen $z = a + bi$ és $w = c + di$. Ekkor $\overline{zw} = (ac - bd) - (ad + bc)i = \overline{z}\,\overline{w}$.

1.3.10.

(1) Igaz, azt kell belátni, hogy $\overline{z - w} = \overline{z} - \overline{w}$. Ez közvetlenül kiszámolható. Második megoldásként vegyük észre, hogy az összegtartás miatt $\overline{z - w} = \overline{z} + (\overline{-w})$. Így elég megmutatni, hogy a konjugálás az ellentettképzést tartja, azaz hogy $\overline{-w} = -\overline{w}$. Legyen $u = -w$, akkor ismét az összegtartás miatt $0 = \overline{0} = \overline{u + w} = \overline{u} + \overline{w}$, amiből az állítás következik.

(2) Nem igaz, például $|1 + (-1)| \neq |1| + |-1|$.

(3) Igaz, és bizonyítás teljesen analóg az (1)-beli második megoldással. Tekintsük a z/w hányadost, és legyen $u = 1/w$. A szorzattartás miatt $|z/w| = |zu| = |z||u|$. Másfelől $uw = 1$ miatt $|u||w| = 1$, és így $|z|/|w| = |z||u| = |z/w|$.

1.4. A komplex számok trigonometrikus alakja.

1.4.1. Az világos, hogy $r = s \neq 0$, mert mindkettő $|z|$-kel egyenlő. Az egyenlőség mindkét oldalát szorozzuk be $\cos(-\alpha) + i\sin(-\alpha)$-val. Ekkor a szorzat képlete miatt

$$\cos(\alpha - \alpha) + i\sin(\alpha - \alpha) = \cos(\beta - \alpha) + i\sin(\beta - \alpha)$$

adódik. A valós és képzetes részeket összehasonlítva $\cos(\beta - \alpha) = 1$ és $\sin(\beta - \alpha) = 0$, ahonnan az állítást kapjuk. (Mindez geometriailag is látszik, hiszen egyenlő komplex számok hossza és szöge is egyenlő.) A megfordítás nyilvánvaló.

1.4.2. Legyen $z = r(\cos\alpha + i\sin\alpha)$ és $w = s(\cos\beta + i\sin\beta)$. Olyan u számot keresünk, amit w-vel megszorozva z-t kapunk. Keressük u-t is trigonometrikus alakban, azaz legyen $u = t(\cos\gamma + i\sin\gamma)$. Ekkor

$$r(\cos\alpha + i\sin\alpha) = z = uw = ts(\cos(\gamma + \beta) + i\sin(\gamma + \beta))\,.$$

A trigonometrikus alak egyértelműségéből következik, hogy $r = st$, és $\alpha = \beta + \gamma$ (pontosabban $\alpha - (\beta + \gamma)$ a 360° egész számú többszöröse). Ezért

$$w/z = (r/s)(\cos(\alpha - \beta) + i\sin(\alpha - \beta))\,.$$

Vagyis a hosszokat osztani kell, a szögeket pedig kivonni (modulo 360°).

1.4.3. A $\overline{z}$ a z tükörképe a valós tengelyre. A $z-w$ az a vektor, ami a w pontból a z pontba mutat, ennek abszolút értéke pedig a hossza, vagyis *a z és w távolsága.*

1.4.4. Az ilyen feladatok megoldásának kétféleképpen vághatunk neki. Megpróbálhatjuk, hogy z helyébe $x+yi$-t helyettesítünk. A műveletek elvégzése után olyan összefüggést kapunk x és y között, amit koordináta-geometriai módszerekkel érthetünk meg, például ráismerhetünk egy egyenes, vagy egy kör egyenletére. Ez a módszer azonban sok számolással jár. Ezért előbb érdemes meggondolni, hogy a feladatból nem olvashatunk-e le közvetlenül geometriai jelentést. Ha sikerül, akkor általában elegáns megoldást kapunk.

(1) Ha $z=x+yi$, akkor $z+3+2i=x+yi+3+2i=(x+3)+(y+2)i$. Mivel $x+3$ és $y+2$ valós számok, ennek a számnak a valós része $x+3$. Tehát az $x+3\le -2$ egyenlőtlenséget kapjuk. Innen $x\le -5$, tehát a keresett alakzat egy félsík, amelyet az $x=-5$ egyenletű függőleges egyenes határol.
(2) Ha $z=x+yi$, akkor $x+1\ge y-3$ adódik, vagyis $y\le x+4$. Ez is egy (zárt) félsík, ami az $y=x+4$ egyenes alatt lévő pontokból áll, az egyenest is beleértve.
(3) Ha koordináta-geometriára vezetjük vissza az állítást egy kör egyenletét kell felismernünk. Jobb azonban, ha közvetlenül okoskodunk. A $|z-1-i|$ szám az előző feladat szerint a z és $1+i$ pontok távolsága. Az egyenlőtlenség tehát azt fejezi ki, hogy a z pont az $1+i$ ponttól legfeljebb 3 egység távolságra van. Vagyis egy zárt körlapot kapunk, melynek sugara 3, középpontja $(1,1)$.
(4) Ugyancsak az előző feladat szerint ez azon z pontok halmaza, amelyek a $3-2i$ és a $-4+i$ pontoktól egyenlő távolságra vannak, azaz a két pontot összekötő szakasz felező merőlegese.
(5) Ez koordináta-geometriával egyszerűbb. Mondhatjuk azonban a következőt is: a $\overline{z}$ a z tükörképe a valós tengelyre. Ha e két vektor összege -1, akkor egy rombuszt kapunk, mely átlójának két végpontja 0 és -1. A lehetséges csúcsok tehát a $\mathrm{Re}(z)=-1/2$ függőleges egyenesen vannak.
(6) Az első halmaznál $|z|^2=z\overline{z}=1$, tehát az egységkört kapjuk. A második halmaz esetében átszorzással $1+8z=|z|^2$ adódik. Mivel $|z|$ valós, z is az, és így $|z|^2=z^2$. A másodfokú egyenletet megoldva $z=4\pm\sqrt{17}$ adódik.
(7) Mivel $r=|z|$ nemnegatív valós, $iz=r$-et i-vel osztva $z=-ir$ adódik, azaz a keresett halmaz a képzetes tengely negatív része a nullával együtt. Ennek minden pontja jó, mert $|-ir|=r$.
(8) Végezzük el az osztást a $(z-1)/(z+1)$ tört esetében, azaz szorozzunk be a nevező konjugáltjával. Ekkor a számláló értéke $(z-1)(\overline{z}+1)=(|z|^2-1)+(z-\overline{z})$. Itt $|z|^2-1$ valós, $z-\overline{z}$ pedig tisztán képzetes. Tehát a $(z-1)/(z+1)$ valós része akkor és csak akkor nulla, ha $|z|=1$, a képzetes része pedig akkor nulla, ha $z=\overline{z}$, vagyis ha z valós. Vagyis az első halmaz az egész valós egyenes, kivéve a -1 számot, a második halmaz pedig az egész egységkör, szintén kivéve a -1 számot.

1.4.5. Konkrét szám esetében a $z = a+bi$ trigonometrikus alak felírásához először érdemes azt meggondolni, hogy z szám melyik síknegyedbe esik, ezt a és b előjele dönti el. Ezután a $|z| = \sqrt{a^2+b^2}$ és a $\operatorname{tg}\alpha = b/a$ összefüggésből már könnyen megkapjuk a trigonometrikus alakot. Vigyázzunk, a $\cos\alpha - i\sin\alpha$ szám nincs trigonometrikus alakban, ennek szöge ugyanis $-\alpha$ (vagyis $2\pi - \alpha$). Az eredmények:

(1) $1+i = \sqrt{2}(\cos 45^\circ + i\sin 45^\circ)$ és $1-i = \sqrt{2}(\cos 315^\circ + i\sin 315^\circ)$.
(2) $\sqrt{3}+i = 2(\cos 30^\circ + i\sin 30^\circ)$ és $-1-\sqrt{3}i = 2(\cos 240^\circ + i\sin 240^\circ)$.
(3) $\cos 300^\circ + i\sin 300^\circ$.
(4) $(\sqrt{6}/2)(\cos 315^\circ + i\sin 315^\circ)$.

1.4.6.

(1) Az origóból való háromszorosra nyújtás, majd eltolás az x-tengely pozitív felének irányába két egységgel.
(2) Forgatva nyújtás az origóból: 45°-kal forgatunk és $\sqrt{2}$-szeresre nyújtunk. Ez az $1+i$ trigonometrikus alakjából olvasható le.
(3) A z pont képe a z-t az origóval összekötő félegyenesen van, és távolsága az origótól a z távolságának reciproka.

Ezt a transzformációt a geometriában az egységkörre vonatkozó *inverziónak* nevezik. Nevezetes tulajdonsága, hogy kört és egyenest is körbe vagy egyenesbe visz. Hasonló tulajdonságúak a $z \mapsto (az+b)/(cz+d)$, úgynevezett *törtlineáris transzformációk* is.

1.4.7.

(1) $(z+w)/2$. Ez leolvasható például az 1.4.1. ábráról, hiszen a paralelogramma átlói felezik egymást.
(2) $\{x \in \mathbb{C} : |x-z| = |x-w|\}$.
(3) $\{x \in \mathbb{C} : |x-z| = |w-z|\}$.
(4) iz.
(5) $i(z-w)$.
(6) A $z-w$ vektort kell $+90^\circ$-kal elforgatni, majd a kezdőpontját a w-be tenni, ami azt jelenti, hogy a végpontja (az origótól számítva) $i(z-w)+w$-ben lesz.
(7) Ha x a keresett pont, akkor az x-ből z-be mutató vektor $\pm 90^\circ$-kal történő elforgatottja x-ből w-be kell, hogy mutasson. Vagyis $(z-x)i = w-x$, illetve $(z-x)(-i) = w-x$. Innen x-re $(w-zi)/(1-i)$, illetve $(w+zi)/(1+i)$ adódik.
(8) Legyen $\varepsilon = \cos 120^\circ + i\sin 120^\circ$, ekkor $\varepsilon^2 = \overline{\varepsilon} = \cos 240^\circ + i\sin 240^\circ$. Az előzőhöz hasonló számolással $(w-\varepsilon z)/(1-\varepsilon)$, illetve $(w-\varepsilon^2 z)/(1-\varepsilon^2)$ adódik.

1.4.8. A négyzet négy csúcsa legyen A, B, C, D, pozitív körüljárás szerint. Ekkor az AB oldalra kifelé írt négyzet középpontja az előző feladat (7) pontjának megoldását felhasználva $(B + Ai)/(1 + i)$. A másik három négyzet középpontját ugyanígy kapjuk. A szemközti négyzetek középpontját összekötő két vektor tehát

$$\frac{1}{1+i}\big((B + Ai) - (D + Ci)\big)\,,$$

illetve

$$\frac{1}{1+i}\big((C + Bi) - (A + Di)\big)\,.$$

Az első vektor i-szerese a második, ezért a két vektor egyenlő hosszú, és merőleges.

1.4.9. Legyen $\varepsilon = \cos 120^\circ + i \sin 120^\circ$ és $\eta = \cos 60^\circ + i \sin 60^\circ$. A szabályos hatszöget felrajzolva látjuk, hogy $\eta = 1 + \varepsilon$ és $1 + \varepsilon + \varepsilon^2 = 0$, továbbá nyilván $\eta^2 = \varepsilon$ és $\varepsilon\eta = -1$. Ha a háromszög csúcsai A, B, C, akkor az 1.4.7. Gyakorlat (8) pontja miatt az AB csúcsra kifelé írt szabályos háromszög középpontja

$$X = \frac{1}{1-\varepsilon}(A - \varepsilon B)\,.$$

Analóg módon írhatjuk fel a másik két szabályos háromszög középpontját is, jelölje ezeket Y és Z. Azt kell belátni, hogy az $\overrightarrow{XY}$ vektort 60°-kal elforgatva az $\overrightarrow{XZ}$-t kapjuk, azaz $(Y - X)\eta - (Z - X) = 0$. Behelyettesítve, $1 - \varepsilon$-nal szorozva, és A, B, C szerint rendezve a következőt kapjuk:

$$A(-\eta + \varepsilon + 1) + B(\eta + \varepsilon\eta - \varepsilon) + C(-\varepsilon\eta - 1)\,.$$

A fenti összefüggések miatt itt A, B és C együtthatója is nulla.

1.4.10. Csak a megoldás ötletét mondjuk el, a diszkussziót az olvasóra hagyjuk. Két komplex szám hányadosának szöge a szögek különbsége. Ez a hányados tehát akkor lesz pozitív valós, ha a két vektor szöge ugyanaz (hiszen a pozitív valós számok szöge 0°), és akkor lesz negatív valós, ha a két vektor iránya ellentétes (hiszen a negatív valós számok szöge 180°). Rögzítsük a z_1 és z_2 pontokat. Ekkor $(z_3 - z_1)/(z_3 - z_2)$ szöge a $z_1z_2z_3$ háromszögnek a z_3-nál levő szöge. A kettősviszony tehát akkor pozitív valós, ha a z_1z_2 szakasz a z_3 és z_4 pontokból ugyanolyan szögben látszik, vagyis ha z_3 és z_4 ugyanazon a látóköríven van. A kettősviszony akkor lesz negatív valós, ha z_3 és z_4 ugyanazon a látókörön van, de ellentétes íveken. Az egyenest azért kell megengedni, mert a vizsgált háromszögek el is fajulhatnak.

1.4.11. Legyenek a négyszög csúcsai A, B, C, D. Ekkor

$$(A - B)(C - D) + (A - D)(B - C) = (A - C)(B - D)\,,$$

hiszen ez azonosság. A háromszög-egyenlőtlenség miatt innen

$$|(A - C)(B - D)| \le |(A - B)(C - D)| + |(A - D)(B - C)|\,.$$

De a baloldalon ef, a jobboldalon $ac + bd$ áll. Egyenlőség akkor van, ha $(A - B)(C - D)$ és $(A - D)(B - C)$ párhuzamos, és egyenlő állású, vagyis ha a hányadosuk pozitív valós

szám. Az előző feladat szerint ilyenkor $ABCD$ húrnégyszög. Megfordítva, ha $ABCD$ konvex húrnégyszög, akkor az A és C csúcsoknál levő szögek összege 180°, ahonnan az előző feladat megoldása szerint következik, hogy $(A-B)(C-D)$ és $(A-D)(B-C)$ hányadosa pozitív valós. A diszkussziót most is az olvasóra hagyjuk.

1.4.12. Legyen $\varepsilon = \cos(x/2) + i\sin(x/2)$, akkor a keresett összeg az $\varepsilon^2 + \varepsilon^4 + \cdots + \varepsilon^{2n}$ képzetes része. A mértani sort összeadva az eredmény

$$\varepsilon^2 \frac{\varepsilon^{2n}-1}{\varepsilon^2-1} = \varepsilon^{n+1} \frac{\varepsilon^n - (1/\varepsilon^n)}{\varepsilon - (1/\varepsilon)}\,.$$

Ez az átírás azért jó, mert $\varepsilon - (1/\varepsilon) = -2i\sin(x/2)$ és $\varepsilon^n - (1/\varepsilon)^n = -2i\sin(nx/2)$. Így

$$\sin x + \sin 2x + \cdots + \sin nx = \frac{\sin((n+1)x/2)\sin(nx/2)}{\sin(x/2)}\,,$$

és

$$\cos x + \cos 2x + \cdots + \cos nx = \frac{\cos((n+1)x/2)\sin(nx/2)}{\sin(x/2)}\,.$$

A végeredmény birtokában természetesen az állítás már komplex számok nélkül is igazolható, például n szerinti indukcióval.

1.5. Egységgyökök és rendjeik.

1.5.1. Az r pozitív valós szám, és az n-edik gyökét is a pozitív valós számok között keressük. Az analízis eredményei szerint ilyen n-edik gyök mindig pontosan egy van.

1.5.2. Keressük az n-edik gyököket $w = s(\cos\beta + i\sin\beta)$ alakban, ekkor

$$w^n = s^n(\cos n\beta + i\sin n\beta) = r(\cos\alpha + i\sin\alpha)\,,$$

ahonnan a trigonometrikus alak egyértelműsége miatt $s = \sqrt[n]{r}$, és $n\beta - \alpha = 2k\pi$, ahol k egész szám. A k számot helyettesíthetjük az n-nel való osztási maradékával, mert ez a $\beta = (\alpha + 2k\pi)/n$ szöget csak modulo 2π változtatja meg.

1.5.3. Ha $|z| > 1$, akkor $1 < |z| < |z|^2 < |z|^3 < \ldots$ egyre nagyobb lesz, soha nem lesz közöttük egyenlő. Sőt a negatív kitevőkre sem, mert $1 = |z|^0 > |z|^{-1} > \ldots$ meg egyre kisebb lesz. Ugyanez a helyzet akkor, ha $|z| < 1$, mert akkor minden fordítva van. (Elegánsabban: a z helyett az $1/z$-re mondható el a fenti gondolatmenet, aminek már 1-nél nagyobb az abszolút értéke, viszont a hatványai ugyanazok, mint a z hatványai.) Tehát csak $|z| = 1$ jön szóba, vagyis $z = 1$ vagy -1. Az 1 hatványai egyesével, a -1 hatványai kettesével ismétlődnek. Valójában az 1 első, a -1 második egységgyök.

1.5.4. Képzeljük azt, hogy kettesével ugrál. Ha n páratlan, akkor az első körben pont átugorja a kiindulópontot, és így n lépést megtéve, minden csúcsot érintve, két kör után ér haza. Ha viszont az n páros, akkor már $n/2$ lépés, és egy kör megtétele után hazaér, miközben a csúcsok felét kihagyja.

Általában, ha k-asával ugrál, akkor m lépést megtéve a km-edik csúcson lesz. Ez akkor a kiindulópont, ha $n \mid km$. A legkisebb ilyen m számot keressük. Nyilván

$$n \mid km \iff \frac{n}{(n,k)} \,\Big|\, \frac{k}{(n,k)} m$$

(itt az (n,k) legnagyobb közös osztót jelöl). Mivel $n/(n,k)$ és $k/(n,k)$ relatív prímek, ez az oszthatóság akkor és csak akkor érvényes, ha

$$\frac{n}{(n,k)} \,\Big|\, m\,.$$

A *legkisebb* ilyen (pozitív) m természetesen maga az $n/(n,k)$. Ezért a bolha ennyi lépést tesz meg, amikor először visszaér (és ennyi csúcsot is érint). Ezalatt k-szor ennyi „távolságot" tesz meg, és mivel a kör hossza n, a megtett körök száma a megtett távolság n-edrésze, vagyis $k/(n,k)$.

Megjegyezzük, hogy a fenti gondolatmenet negatív egész k számokra is érvényes, ebben az esetben a bolha visszafelé ugrál.

1.5.5. A megoldáshoz felhasználjuk a gyökvonás képletét (1.5.2. Gyakorlat). Néhány esetben egyszerűbb csak egy gyököt megkeresni, és azt az egységgyökökkel végigszorozni.

(1) A harmadik egységgyökök, algebrai alakban 1 és $-1/2 \pm i\sqrt{3}/2$.
(2) A -4 trigonometrikus alakja $4(\cos 180^\circ + i \sin 180^\circ)$. A negyedik gyökök $\pm 1 \pm i$.
(3) $\sqrt{3} - i = 2(\cos 330^\circ + i \sin 330^\circ)$, a képlet szerint a 8-adik gyökök hossza $\sqrt[8]{2}$, szögeik $41, 25^\circ + k \cdot 45^\circ$, ahol $0 \le k < 8$.
(4) Ezek azok a $2n$-edik egységgyökök, amelyek nem n-edik egységgyökök. Szögeik a $2\pi/2n$ páratlan többszörösei, hosszuk 1.

1.5.6. Elég meghatározni a rendeket, mert ezután a válasz a következő gyakorlat megoldásából leolvasható. Az 1.5.6. Állítást használjuk. Az $1 + i$ és a $\cos(\sqrt{2}\pi) + i \sin(\sqrt{2}\pi)$ rendje végtelen, az $(1+i)/\sqrt{2}$ szöge $360^\circ/8$, tehát rendje 8, végül $\cos(336^\circ) + i \sin(336^\circ)$ rendje a $336/360$ tört egyszerűsített alakjának nevezője, azaz 15.

1.5.7. Ha egy egységgyök rendje d, akkor csak az $n = d$ esetben lesz primitív n-edik egységgyök, és pontosan a $d \mid n$ számokra lesz lesz n-edik egységgyök, hiszen ezek a jó kitevői.

1.5.8. Ha $\varepsilon^n = i$, akkor $\varepsilon^{4n} = i^4 = 1$, ezért ε rendje véges, és $4n$-nek osztója. Ha $o(\varepsilon) = d$, akkor $\varepsilon^d = 1$. Innen $1 = \varepsilon^{dn} = i^d$, és így $4 = o(i) \mid d$.

1.5.9. Mivel $\varepsilon^{512} = 1$, ezért $(-i\varepsilon)^{512} = 1$. Így $o(-i\varepsilon) \mid 512$. De $512 = 2^9$, tehát ha $o(-i\varepsilon) \neq 512$, akkor már $o(-i\varepsilon) \mid 256$ is teljesül. De ez lehetetlen, mert $(-i\varepsilon)^{256} = \varepsilon^{256}$, ami nem 1, mert 512 a legkisebb pozitív jó kitevője ε-nak. Tehát $o(-i\varepsilon) = 512$.

Második megoldás. Az 1.5.6. Állítást fogjuk használni. Az ε szám szöge 360°-nak $k/512$-szerese, ahol $(k, 512)$=1, vagyis k páratlan. Mivel $-i$ szöge 360°-nak $-1/4$-szerese, ezért $-i\varepsilon$ szöge 360°-nak $(k/512)-(1/4) = (k-128)/512$-szöröse. Ez egyszerűsíthetetlen tört, hiszen a nevező 2-hatvány, a számláló pedig páratlan. Ezért $-i\varepsilon$ rendje is 512.

1.5.10. Ha ε rendje 4-gyel osztható, akkor $o(-\varepsilon) = o(\varepsilon)$. Ha csak kettővel osztható, de 4-gyel nem, akkor $o(-\varepsilon) = o(\varepsilon)/2$. Végül ha $o(\varepsilon)$ páratlan, akkor $o(-\varepsilon) = 2 \cdot o(\varepsilon)$. Minderre két bizonyítást is adunk. Legyen $o(\varepsilon) = n$.

Első megoldás. Keressük meg a $-\varepsilon$ jó kitevőit. Nyilván $(-\varepsilon)^k = (-1)^k\varepsilon^k$. Ez akkor lesz 1, ha $\varepsilon^k = (-1)^k$. Speciálisan $k = 2n$ jó kitevő. Négyzetre emelve $\varepsilon^{2k} = 1$, azaz $n \mid 2k$ minden k jó kitevőre. Vagyis ha $d = o(-\varepsilon)$, akkor $n \mid 2d$ és $d \mid 2n$. Tehát $nx = 2d$ és $dy = 2n$ alkalmas x, y pozitív egészekre, ahonnan $xy = 4$ adódik. Így d/n (ami $x/2$) csak 1, 2, vagy $1/2$ lehet.

Ha n páratlan, akkor innen $n \mid d$, és mivel n nem jó kitevő ilyenkor, $d = 2n$. Ha n páros, akkor már n is jó kitevő, tehát $d \mid n$, és így az a kérdés, hogy $n/2$ mikor jó kitevő. Nyilván $(\varepsilon)^{n/2} = -1$ (mert $(\varepsilon)^{n/2}$ négyzete 1, de önmaga nem 1). Tehát $n/2$ akkor jó kitevő, ha $(-1)^{n/2} = -1$, azaz ha $4 \nmid n$. Ilyenkor $d = n/2$, különben csak $d = n$ lehet.

Második megoldás. Ismét az 1.5.6. Állítást használjuk. Legyen ε szöge 360°-nak k/n-szerese, ahol $(k, n) = 1$. Mivel -1 szöge 360°/2, a $-\varepsilon$ szöge 360°-nak $(k/n) + (1/2) = (2k + n)/(2n)$-szerese. Azt kell megvizsgálnunk, hogy ennek a törtnek mennyi a nevezője az egyszerűsítés után. Könnyű meggondolni, hogy a számlálónak és a nevezőnek nem lehet 2-től különböző prímosztója. Tehát az a kérdés, hogy a 2 melyik hatványával lehet egyszerűsíteni. Ha n páratlan, akkor már 2-vel sem lehet egyszerűsíteni, mert a számláló páratlan. Ha n páros, akkor $(k, n) = 1$ miatt k páratlan. Ilyenkor 2-vel lehet egyszerűsíteni, és a számláló $k + n/2$ lesz. Ha $4 \mid n$, akkor ez páratlan, tehát nem lehet tovább egyszerűsíteni. Ha $4 \nmid n$, akkor még 2-vel egyszerűsíthetünk, de tovább már nem, a nevező miatt.

1.5.11. Az első esetben a tizenkettedik egységgyököket kapjuk, mindegyiket kétszer. A másodikban a negyvenkettedik egységgyököket kapjuk, mindegyiket egyszer.

1.5.12.

(1) A közös gyökök azok az ε számok, melyekre $\varepsilon^n = 1 = \varepsilon^m$, vagyis amelyek rendje osztója m-nek is és n-nek is. Ezek tehát pontosan az (m, n)-edik egységgyökök, így számuk (m, n).

(2) Ha $\varepsilon^m = 1$ és $\eta^n = 1$, akkor nyilván $(\varepsilon\eta)^{mn} = 1$.

(3) Legyen $o(\varepsilon) = m$ és $o(\eta) = n$. Ha m és n nem relatív prímek, akkor legkisebb közös többszörösük, amit $[m, n]$ jelöl, kisebb, mint a szorzatuk. De $(\varepsilon\eta)^{[m,n]} = 1$, tehát $\varepsilon\eta$ rendje kisebb, mint mn.

Tegyük most fel, hogy m és n relatív prímek. Legyen $d = o(\varepsilon\eta)$, be kell látni, hogy $d = mn$. A (2) miatt ehhez elég, hogy $mn \mid d$, ehhez pedig, hogy $m \mid d$

és $n \mid d$ (hiszen m és n relatív prímek). Szimmetriaokokból elég csak az első oszthatóságot megmutatni.

Nyilván $(\varepsilon\eta)^d = 1$. Ezt n-edik hatványra emelve $1 = \varepsilon^{nd}\eta^{nd} = \varepsilon^{nd}$. Ezért $m = o(\varepsilon) \mid nd$. Mivel $(n, m) = 1$, ebből következik a kívánt állítás.

1.5.13. Elsőnek az n-edik egységgyökök összegét számítjuk ki. Hogyan fogná fel ezt a feladatot egy fizikus? Azt mondaná, hogy egy szabályos sokszög csúcsaiba mutató vektorok s átlaga a súlypontba, vagyis a sokszög középpontjába mutat. Azért a középpontjába, mert a sokszög szimmetrikus. Ha nem a középpontba mutatna, akkor el lehetne forgatni a sokszöget úgy, hogy önmagába menjen, de s elforduljon, ami lehetetlen.

Második megoldásként ezt a gondolatmenetet modellezzük algebrailag. Jelölje S az n-edik egységgyökök összegét, és legyen ε az az egységgyök, melynek szöge $2\pi/n$. Ezzel a szöggel „forgassuk el" az S összeget, azaz szorozzuk meg ε-nal. Ekkor az összeg tagjai ugyanazok maradnak, csak más sorrendben lesznek felírva. Ezért $S\varepsilon = S$. Innen $S = 0$ vagy $\varepsilon = 1$ következik. De $\varepsilon = 1$ pontosan akkor, ha $n = 1$. Tehát a keresett összeg nulla, kivéve ha $n = 1$, amikor az összeg értéke 1.

Amikor az n-edik egységgyökök szorzatát vizsgáljuk, akkor másik ötlet segít. Párosítsuk mindegyik egységgyököt a konjugáltjával. Ez azért hasznos, mert $\varepsilon\overline{\varepsilon} = |\varepsilon|^2 = 1$, vagyis a konjugáltak kiejtik egymást. Marad azoknak az egységgyököknek a szorzata, amelyeknek a párja önmaga, azaz amelyek valósak. Ilyen egységgyök csak az 1 és a -1 lehet. Ha n páros, akkor a -1 is szerepel az n-edik egységgyökök között, ezért az eredmény -1. Ha n páratlan, akkor viszont 1 a keresett szorzat értéke.

Megjegyezzük, hogy az egységgyökök összegét és szorzatát is kiszámolhattuk volna közvetlenül a trigonometrikus alakból. Az összeghez mértani sort kell összeadni, a szorzásnál meg a szögek adódnak össze, és itt számtani sort kapunk. Ez a módszer hasznos a négyzetösszeg kiszámítására is. A mértani sor összegképlete alapján

$$\varepsilon_1^2 + \varepsilon_2^2 + \cdots + \varepsilon_n^2 = \varepsilon_1^2 + \varepsilon_1^4 + \cdots + \varepsilon_1^{2n} = \frac{\varepsilon_1^{2n} - 1}{\varepsilon_1^2 - 1}\,.$$

A számláló nulla, és így az eredmény is az, kivéve ha a nevezőben nulla van, vagyis ha $\varepsilon_1^2 = 1$. Ez csak úgy lehet, ha $n = 1$ vagy $n = 2$. Ezekben az esetekben közvetlenül láthatjuk, hogy a négyzetösszeg 1, illetve 2.

1.5.14. A binomiális tételt alkalmazzuk először az $(1 + 1)^n$ összegre.

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}\,.$$

Hasonlóan felírva az $(1 - 1)^n$ összeget, azt kapjuk, hogy

$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n\binom{n}{n}\,.$$

Legyen

$$A = \binom{n}{0} + \binom{n}{2} + \dots \qquad \text{és} \qquad B = \binom{n}{1} + \binom{n}{3} + \dots$$

(az összegezést akár a végtelenségig is folytathatjuk, mert egy binomiális együttható értéke nulla lesz, ha az alul álló szám már meghaladja a felül állót). Ekkor a fenti képletek szerint $A + B = 2^n$ és $A - B = 0$, vagyis $A = B = 2^{n-1}$. Végül írjuk fel az $(1+i)^n$ összeget.

$$(1+i)^n = \binom{n}{0} + i\binom{n}{1} - \binom{n}{2} - i\binom{n}{3} + \binom{n}{4} + i\binom{n}{5} - \binom{n}{6} - i\binom{n}{7} + \binom{n}{8} \dots .$$

Ezért

$$\mathrm{Re}((1+i)^n) = \binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \binom{n}{6} + \binom{n}{8} - + \dots .$$

Ha most

$$X = \binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \dots \qquad \text{és} \qquad Y = \binom{n}{2} + \binom{n}{6} + \binom{n}{10} + \dots ,$$

akkor $X - Y = \mathrm{Re}((1+i)^n)$ és $X + Y = B = 2^{n-1}$. Innen pedig a keresett X kifejezhető: $X = (2^{n-1} + \mathrm{Re}((1+i)^n))/2$. Az $(1+i)^n$ értékét trigonometrikus alakban számíthatjuk ki, az eredmény $2^{n/2}(\cos(2n\pi/8) + i\sin(2n\pi/8))$, aminek a valós része $2^{n/2}\cos(2n\pi/8)$. A feladatban $n = 1867$, így a végeredmény $X = 2^{1865} - 2^{932}$.

1.5.15. Egyrészt

$$(\cos x + i\sin x)^n = \cos(nx) + i\sin(nx)\,,$$

másrészt a binomiális tétel miatt

$$(\cos x + i\sin x)^n = \sum_{j=0}^{n} i^j \binom{n}{j} \cos^{n-j} x \sin^j x$$

(az itt használt, úgynevezett szumma jelölés magyarázata a 2.1.6. Definícióban található). Innen valós és képzetes részt véve

$$\cos(nx) = \cos^n x - \binom{n}{2}\cos^{n-2} x \sin^2 x + \binom{n}{4}\cos^{n-4} x \sin^4 x - \binom{n}{6}\cos^{n-6} x \sin^6 x \dots$$

(itt $\sin^2 x$ helyére $1 - \cos^2 x$-et írva $\sin x$ teljesen eltüntethető), és

$$\sin(nx) = \binom{n}{1}\cos^{n-1} x \sin x - \binom{n}{3}\cos^{n-3} x \sin^3 x + \binom{n}{5}\cos^{n-5} x \sin^5 x \dots$$

11.2. Polinomok

2.1. A polinom fogalma.

2.1.1. Az eredmény

$$a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 +$$
$$+(a_0b_3 + a_1b_2 + a_2b_1)x^3 + (a_1b_3 + a_2b_2)x^4 + a_2b_3x^5 .$$

Amennyiben a_2 és b_3 sem nulla, a szorzat foka 5.

2.1.2. Először a baloldali zárójelet bontjuk föl:

$$(a_1 + \cdots + a_n)(b_1 + \cdots + b_m) = a_1(b_1 + \cdots + b_m) + \cdots + a_n(b_1 + \cdots + b_m) .$$

Ha most mindegyik zárójelben beszorzunk, az állítást kapjuk.

2.1.3. Az eredmények

$$(x^3 + 3x^2 + 2) - (x^3 + 3x - 4) = 3x^2 - 3x + 6 ,$$
$$(x^2 + ix + 3)(x^2 + i) = x^4 + ix^3 + (3 + i)x^2 - x + 3i .$$

Az első polinom másodfokú, a második negyedfokú.

2.1.4. Ha $n = 3$, akkor az eredmény

$$a_1a_2a_3 + a_1a_2b_3 + a_1b_2a_3 + a_1b_2b_3 + b_1a_2a_3 + b_1a_2b_3 + b_1b_2a_3 + b_1b_2b_3 .$$

Az általános $(a_1 + b_1) \ldots (a_n + b_n)$ szorzatot több lépésben fejthetjük ki (és közben mindig felhasználhatjuk a 2.1.2. Gyakorlatot). A végeredmény egy 2^n tagú összeg lesz, amelynek mindegyik tagja egy n-tényezős $x_1x_2 \ldots x_n$ szorzat, ahol az x betű helyére a vagy b betűt kell írni az összes lehetséges kombinációban. Általában *ha több soktagú összeget szorzunk össze, akkor mindegyik tényezőből ki kell venni egy tagot az összes lehetséges módon egymástól függetlenül, ezeket össze kell szorozni, és a kapott szorzatokat összeadni.*

2.1.5. Írjuk be az a_{ij}-ket egy táblázatba: az a_{ij} az i-edik sor j-edik helyére kerüljön (tehát n sor lesz, és m oszlop). Ekkor mindkét szumma a táblázatban álló számok összege, csak az elsőben először az oszlopokat adjuk össze, a másodikban pedig először a sorokat.

2.2.1. A tényezők száma szerinti indukcióval bizonyítunk, azaz feltesszük, hogy az n-nél kevesebb tényezős szorzatok értéke már független a zárójelezéstől. Ha adott egy n-tényezős szorzat, akkor az $A * B$ alakú, ahol A és B már rövidebb szorzatok. Ha A nem egytényezős, akkor az indukciós feltevés miatt $A = a_1 * C$ alakban írható. Az asszociativitást alkalmazva $A * B = (a_1 * C) * B = a_1 * (B * C)$. Vagyis mindegyik n-tényezős szorzat $a_1 * D$ alakra hozható. Az indukciós feltevés miatt D értéke független a zárójelezéstől, tehát tényleg bármely két zárójelezés ugyanazt az eredményt adja.

2.2. A szokásos számolási szabályok.

2.2.2. Legyenek f, g, h az X halmazon értelmezett, X-be vezető függvények. Azt kell belátni, hogy $f \circ (g \circ h) = (f \circ g) \circ h$. Két függvény akkor egyenlő, ha minden helyen megegyezik az értékük. De ha $x \in X$ tetszőleges, akkor a kompozíció definícióját ismételten felhasználva

$$\big(f \circ (g \circ h)\big)(x) = f\big((g \circ h)(x)\big) = f\Big(g\big(h(x)\big)\Big),$$

és

$$\big((f \circ g) \circ h)\big)(x) = \big(f \circ g\big)\big(h(x)\big) = f\Big(g\big(h(x)\big)\Big).$$

A két érték tehát tényleg ugyanaz.

Ha vesszük az x-tengelyre való T tengelyes tükrözést, illetve az origó körüli 90 fokos F forgatást, akkor ez a két transzformáció nem cserélhető fel. Ezt a legegyszerűbben komplex számokkal láthatjuk be: $T(z) = \overline{z}$, és $F(z) = iz$, de $(T \circ F)(z) = \overline{iz} = -i\overline{z}$ nem egyenlő $(F \circ T)(z) = i\overline{z}$-tal, kivéve ha $z = 0$.

2.2.3. Az útmutatásban szereplő állítás igazolása a következő. Keressük meg azt a könyvet, ami a legbaloldalra való, és addig cseréljük meg mindig a baloldali szomszédjával, amíg a helyére nem kerül. Ezután ugyanezt végigcsináljuk a balról második helyre való könyvvel, és így tovább.

Ha adott az $a_1 * \cdots * a_n$ szorzat, akkor a 2.2.1. Feladat miatt a zárójelezéssel nem kell foglalkoznunk, a kommutativitás viszont lehetővé teszi bármely két szomszédos tényező cseréjét. Ennek ismételgetésével pedig a tényezők bármelyik sorrendje megkapható.

2.2.4. Az *identikus leképezés*, az az *id* függvény, amely X minden eleméhez saját magát rendeli. Nyilvánvalóan $f \circ id = id \circ f = f$ tetszőleges f függvényre (aki nem hiszi, helyettesítsen be tetszőleges $x \in X$-et). Más függvény nem lehet neutrális elem. Ha ugyanis e ilyen, akkor az $e \circ id = id$ egyenletbe x-et helyettesítve $e(x) = x$ adódik.

2.2.5. Ha e baloldali, f jobboldali neutrális elem, akkor $e * f = f$ (mert e baloldali neutrális elem), ugyanakkor $e * f = e$ (mert f jobboldali neutrális elem). Tehát $e = f$. Vagyis ha van baloldali, és van jobboldali neutrális elem is, akkor mindkét fajtából csak egy lehet, és az kétoldali neutrális elem lesz.

2.2.6.

(1) Tegyük fel, hogy v balinverze, és w jobbinverze u-nak. A $*$ asszociativitása miatt $v * (u * w) = (v * u) * w$. De $v * (u * w) = v * e = v$, és $(v * u) * w = e * w = w$. Ezért $v = w$.

(2) Ha u inverze u^{-1} és v inverze v^{-1}, akkor $u * v$ (kétoldali) inverze $v^{-1} * u^{-1}$ lesz. Valóban, $u * v * v^{-1} * u^{-1} = u * e * u^{-1} = e$, és $v^{-1} * u^{-1} * u * v = v^{-1} * e * v = e$.

2.2.7. Ha egy H részhalmaz teljesíti a felsorolt tulajdonságokat, akkor maga is csoport G műveletére nézve (hiszen az asszociativitás azonosság, ami öröklődik G-ből H-ra, a többi csoporttulajdonságot pedig felsoroltuk). Megfordítva, ha H maga is csoport a G műveletére nézve, akkor a G műveletének értelmezve kell lennie H-ban is, azaz (1) teljesül. A többi állításhoz elég belátni, hogy G és H neutrális eleme ugyanaz, és egy h-beli elem inverze H-ban kiszámítva ugyanaz lesz, mint ha G-ben számítanánk ki.

Legyen a H csoport egységeleme f, a G csoporté e. Jelölje f^{-1} az f elemnek a G csoportbeli inverzét. Ekkor $f * f = f$, mert f egységeleme H-nak. Ezért $(f * f) * f^{-1} = f * f^{-1} = e$. Ugyanakkor $f * (f * f^{-1}) = f * e = f$, hiszen e egységeleme G-nek. Az asszociativitás miatt tehát $e = f$. Az, hogy az inverzképzés ugyanaz H-ben, mint G-ben, az inverz egyértelműségéből következik (2.2.6. Feladat), hiszen egy H-beli elem H-beli inverze nyilván inverz G-ben is (mert $e = f$).

2.2.8. Tegyük fel először, hogy a szereplő m és n kitevők pozitívak. Ekkor a (2), (3), (4) állításokat egyszerű leszámlálással tudjuk bizonyítani. Például $a^m a^n$ és a^{m+n} esetében is nyilván $m + n$ darab a betűt írtunk le egymás mellé, $(a^m)^n$ és a^{mn} esetében pedig mn darabot. A (4) állításban a és b egymással szabadon cserélgethető, és nyilván mindkét oldalon n darab a és n darab b szerepel.

Ezután az (1) állítást is be tudjuk látni pozitív n esetén. Azt kell megmutatni, hogy $a^{-n}a^n = e = a^n a^{-n}$. Ha a inverzét b jelöli, akkor az a^{-n} definíció szerint b^n-nel egyenlő. Tudjuk, hogy $ba = e = ab$, azaz a és b felcserélhetők. Ezért a (4) állítás már bizonyított része szerint $a^{-n}a^n = b^n a^n = (ba)^n = e$, és hasonlóan $a^n a^{-n} = e$.

Ha most m és n nulla, vagy negatív is lehet, akkor esetszétválasztással okoskodunk, a negatív kitevőjű hatvány definícióját használva. Példaként a (2) állítást bizonyítjuk, a többi (hasonló) gondolatmenetet az olvasóra hagyjuk.

Ha $m = 0$, akkor $a^m = e$ és $m + n = n$, tehát az állítás tetszőleges egész n-re teljesül. Ha m negatív, mondjuk $m = -k$, ahol k pozitív egész, akkor jelölje ismét b az a inverzét. Ekkor $a^m = a^{-k} = b^k$. Tehát azt kell megmutatni, hogy $b^k a^n = a^{-k+n}$. Ha $n \geq k$, akkor a bal- és a jobboldalon is $n - k$ darab a betű marad (hiszen $ba = e$). Ha viszont $n < k$, akkor a baloldalon $k - n$ darab b betű marad, a jobboldal pedig $a^{-(k-n)}$, ami a negatív kitevőjű hatvány definíciója miatt szintén b^{k-n}.

2.2.9. A disztributivitás (és $0 + 0 = 0$) miatt $0r = (0 + 0)r = 0r + 0r$. Mindkét oldalhoz $0r$ ellentettjét adva $0 = 0r$ adódik. Ugyanígy láthatjuk be, hogy $r0 = 0$ minden r elemre.

Ha u invertálható, azaz $uv = 1$, akkor természetesen u nem lehet nulla, mert akkor $uv = 1$ is nulla lenne. Ekkor tetszőleges r elemre $r = r1 = r0 = 0$, vagyis a gyűrű a nullgyűrű, amit kizártunk az egységelemes gyűrűk közül. Végül

$$0 = r0 = r\big(s + (-s)\big) = rs + r(-s)$$

miatt rs ellentettje, ami definíció szerint $-(rs)$, tényleg $r(-s)$-sel egyenlő. Analóg módon igazolható a $(-r)s = -(rs)$ azonosság is.

2.2.10. Ha az R additív csoportjára alkalmazzuk a 2.2.7. Feladatot, akkor az állítás első felét kapjuk. Ha R test, akkor az R multiplikatív csoportjára (aminek elemei most R nem nulla elemei) is alkalmazhatjuk ezt a feladatot, és akkor az állítás másik felét kapjuk.

2.2.11. Ha $ur = us$, akkor $u(r-s) = 0$. Mivel u nem baloldali nullosztó, innen $r-s = 0$, vagyis $r = s$.

Megjegyezzük, hogy ebben a megoldásban nemcsak a disztributivitást használtuk fel, abból ugyanis csak annyi következne, hogy $u(r-s) = ur + u(-s)$. Szükség volt a 2.2.9. Feladatban bizonyított $u(-s) = -(us)$ összefüggésre is.

2.2.12. Ez pontosan ugyanaz a gondolatmenet, mint a 2.2.14. Tétel bizonyítása. Ha r-nek balinverze s, akkor az $ru = 0$ egyenletet balról s-sel megszorozva $0 = sru = 1u = u$ adódik. Ezért r nem lehet baloldali nullosztó.

2.2.13. Ha u invertálható eleme $\mathbb{Z}_m$-nek, akkor van olyan v, hogy $u *_m v = 1$, vagyis $uv-1$ osztható m-mel. Így u és m minden közös osztója osztja az 1-et is, vagyis u relatív prím az m-hez.

A megfordításhoz legyenek $u_1, \ldots, u_k$ a $\mathbb{Z}_m$-nek az m-hez relatív prím elemei, és u ezek egyike. Ha $u *_m u_j = u *_m u_k$, akkor $m \mid u(u_j - u_k)$. Mivel azonban m és u relatív prímek, innen $m \mid u_j - u_k$, tehát u_j és u_k ugyanazt a maradékot adja m-mel osztva, vagyis ($\mathbb{Z}_m$ elemei lévén) egyenlőek. Beláttuk tehát, hogy $u *_m u_1, \ldots, u *_m u_k$ páronként különbözők. De nyilván $u *_m u_j$ is relatív prím m-hez, tehát az $u *_m u_1, \ldots, u *_m u_k$ számok ugyanazok, mint $u_1, \ldots, u_k$ (csak esetleg más sorrendben). Speciálisan tehát az 1 is szerepel az $u *_m u_j$ számok között, azaz u invertálható.

Ez a bizonyítás elegáns, de némileg csalásnak tekinthető. Kihasználtuk ugyanis a számelmélet relatív prím számokról szóló elemi eredményeit. Márpedig ezek bizonyítása az euklideszi algoritmuson alapszik, amelyből az elsők között következik az, hogy ha u és m relatív prímek, akkor van olyan x és y egész, hogy $ux + my = 1$. Ha ezt szabad használnunk, akkor az x szám mod m maradéka inverze lesz u-nak, tehát a fenti gondolatmenet fölöslegessé válik.

Annak, hogy a fenti megoldást mégis szerepeltettük, két oka van. Egyrészt a relatív prím számok felhasznált tulajdonságai (sőt a számelmélet alaptétele is) ismerős már középiskolából (bár esetleg bizonyítás nélkül), ismerősebb, mint az előző bekezdésben használt állítás. Másrészt a fenti megoldás ötletét általánosítani lehet majd olyan algebrai állítások bizonyítására, ahol a számelméletet már közvetlenül nem alkalmazhatjuk.

2.2.14. A művelet asszociatív, mert $a*(b*c) = a = (a*b)*c$ (sőt, bárhogyan zárójelezünk egy szorzatot, az eredmény mindig a legbaloldali tényező lesz). Nyilván S minden eleme jobboldali neutrális elem. Ha S egyelemű, akkor az egyetlen eleme kétoldali neutrális elem. Ha azonban S legalább kételemű, akkor egyetlen baloldali neutrális eleme sincs.

2.2.15. Ha a megadott halmaz egy gyűrűnek része, és a műveletek is „ugyanazok”, akkor elegendő a 2.2.10. Feladatban megadott tulajdonságokat ellenőrizni. Ezt nagyon sokszor használjuk majd az alábbiakban.

(1) Ez részteste $\mathbb{C}$-nek. Ennek ellenőrzéséhez először is vegyük észre, hogy az összeadás és a szorzás sem vezet ki a megadott halmazból: ha $z = a + bi$ és $w = c + di$ olyan komplex számok, hogy a, b, c, d racionális, akkor

$$z + w = (a + c) + (b + d)i \quad \text{és} \quad zw = (ac - bd) + (ad + bc)i$$

is az adott halmazban van, hiszen $a + c$, $b + d$, $ac - bd$, $ad + bc$ úgyszintén racionális számok. Nyilván a $0 = 0 + 0i$ és az $1 = 1 + 0i$ is a megadott halmazban van (hiszen 0 és 1 is racionális számok). Ha $z = a + bi$ a halmazban van, akkor ellentettje, $(-a) + (-b)i$ is. Végül ha $a + bi \neq 0$, akkor

$$\frac{1}{a + bi} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \,,$$

és ha a, b racionális akkor nyilván $a/(a^2 + b^2)$ és $-b/(a^2 + b^2)$ is racionális. Tehát testről van szó, és ez persze nullosztómentes is. A nullosztómentesség már abból is következik, hogy a $\mathbb{C}$ nullosztómentes, és annak egy részgyűrűjéről van szó.

(2) Ez az előzőhöz mindenben hasonlít, egyetlen kivétellel: a reciprokképzésre kapott képlet kivezet az egész számok közül. Tehát nullosztómentes gyűrűről van szó, amelyben meg kell határoznunk az invertálható elemeket. Ha $a + bi$ invertálható, akkor van olyan $c + di$ ebben a halmazban, hogy $(a + bi)(c + di) = 1$. Szorozzuk meg ezt az egyenlőséget konjugáltjával. A $z\overline{z} = |z|^2$ összefüggés miatt azt kapjuk, hogy $(a^2 + b^2)(c^2 + d^2) = 1$. De mindkét tényező nemnegatív egész szám, és így szorzatuk csak úgy lehet 1, ha mindkettő értéke 1. Tehát $a^2 + b^2 = 1$, és mivel a^2 és b^2 is nemnegatív, ez csak úgy lehet, ha $a = \pm 1$ és $b = 0$, vagy $a = 0$ és $b = \pm 1$. Ekkor az $a + bi$ komplex számra az 1, -1, i, $-i$ értékeket kapjuk. Vagyis csak ezek lehetnek invertálhatók. Ezek tényleg invertálhatók is: 1 és -1 inverze önmaga, az i és a $-i$ pedig egymás inverzei.

(3) Ez is részteste $\mathbb{C}$-nek. A számolás hasonló ahhoz, ahogy az (1)-et oldottuk meg, csak az inverzképzés változik egy kicsit: most a törtet $a - b\sqrt{2}$-vel kell bővíteni:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \,.$$

Ellenőriznünk kell, hogy a nevező csak akkor lehet nulla, ha $a + b\sqrt{2} = 0$. A nevező $(a + b\sqrt{2})(a - b\sqrt{2})$, és noha $\mathbb{C}$ nullosztómentes, ez lehetne nulla akkor is, amikor $a - b\sqrt{2} = 0$. De ebben az esetben $b = 0$, hiszen különben $\sqrt{2} = a/b$ lenne, márpedig $\sqrt{2}$ irracionális szám. De ha $b = 0$, akkor $a = b\sqrt{2} = 0$, és így $a + b\sqrt{2}$ is nulla. Igazából azt láttuk be, hogy az $a + b\sqrt{2}$ egyértelműen meghatározza az a és b racionális számokat.

(4) Ez nem gyűrű, a szorzás nincs jól definiálva, mert kivezet a halmazból. Tegyük fel ugyanis, hogy

$$\sqrt[3]{2}\sqrt[3]{2} = \sqrt[3]{4} = a + b\sqrt[3]{2}$$

alkalmas a és b racionális számokra. Ezt az egyenletet szorozzuk meg $b + \sqrt[3]{2}$-vel, ekkor kiesik a $b\sqrt[3]{4}$, és a rendezés után

$$4 - ab = \sqrt[3]{2}(a + b^2)$$

adódik. Mivel $\sqrt[3]{2}$ irracionális, innen $a + b^2 = 0 = 4 - ab$, ahonnan $b^3 = -4$, ami egyetlen racionális számra sem teljesül. Egy másik, elegáns megoldást mutatunk majd a 3.5.14. Feladatban.

(5) Ez nyilvánvalóan kommutatív gyűrű, aminek nincs egységeleme, és minden nem nulla eleme kétoldali nullosztó.

(6) Ez kommutatív, egységelemes gyűrű, a nullelem az üres halmaz, az egységelem pedig maga az X. Minden a nullától és az egységelemtől különböző elem nullosztó, és így nem is invertálható. Pontosan akkor kapunk testet, ha az X halmaz egyelemű. Erről a gyűrűről lesz még szó a Boole-algebrákról szóló fejezetben.

Ezeket az állításokat könnyen be lehet látni, ha az összeadás és a szorzás definícióját alkalmazzuk. Mintabizonyításként megmutatjuk a disztributivitást, azaz hogy $(A + B)C = AC + BC$. Két halmaz akkor egyenlő, ha kölcsönösen tartalmazzák egymást. Tegyük fel először, hogy $x \in (A + B)C$. Ez azt jelenti, hogy $x \in C$ (hiszen a szorzás a metszetképzés), és $x \in A+B$, vagyis $x \in A$ de $x \notin B$, vagy fordítva, $x \notin A$ de $x \in B$. Az első esetben $x \in AC$ de $x \notin BC$, és így $x \in AC + BC$. A másik esetben $x \notin AC$ de $x \in BC$, és így ismét $x \in AC + BC$. Ezzel beláttuk, hogy $(A + B)C \subseteq AC + BC$. A másik irányú tartalmazás hasonlóan igazolható.

2.2.16. Könnyű ellenőrizni, hogy R zárt a $\mathbb{Z}_6$-beli összeadásra, szorzásra és ellentettképzésre, tehát részgyűrű. Azt gondolhatnánk, hogy mivel az 1 nincs benne, nem lesz egységelemes. De ez nem így van! Ugyanis a 4 egységelem: $4 *_6 4 = 4$, továbbá $4 *_6 2 = 2$ és persze $4 *_6 0 = 0$. Sőt, testet kaptunk, hiszen a 4 és a 2 inverze is önmaga. (A 2.4.16. Feladat megoldásában látni fogjuk, hogy nullosztómentes gyűrűben egy részgyűrű egységeleme csak az eredeti gyűrű egységeleme lehet.)

2.2.17. A (2.1.4.) Gyakorlat szerint $(a+b)^n$ olyan összeg, amelynek tagjai az a és b néhány (összesen n) példányának szorzatai, vagyis $a^{n-j}b^j$ alakúak. Ez a szorzat annyiféleképpen jöhet létre, ahányféleképpen az n darab $(a + b)$ „zárójelből" ki lehet választani azt a j darabot, amelyből b-t választunk (és akkor a többi $n - j$ zárójelből a-t választunk). A C.0.12. Tétel szerint ez $\binom{n}{k}$-féleképpen történhet meg.

A bizonyítás ugyanez tetszőleges kommutatív gyűrű fölött. Ebben az esetben a binomiális együtthatókkal való szorzás azt jelenti, mint bármely egész számmal való szorzás: az elemet ennyi példányban össze kell adni (lásd a 2.2.8. Definíció utáni megjegyzéseket).

2.2.18. A $(\sqrt{2}-1)^n(\sqrt{2}+1)^n = 1$ összefüggésből látszik, hogy $\sqrt{2}+1$ mindegyik hatványa invertálható. Ez végtelen sok különböző szám, hiszen $\sqrt{2}+1 > 1$.

2.2.19. Mivel $\mathbb{Z}_3$ és $\mathbb{Z}_5$ is test, a komplex számoknál látottakhoz hasonlóan világos, hogy ha $a^2+b^2 \neq 0$, akkor $a+bi$ invertálható. A $\mathbb{Z}_3$ mindegyik elemének a négyzete 0 vagy 1, és így $a^2+b^2 = 0$ csak úgy lehet, ha $a = b = 0$. Ezért $\mathbb{Z}_3$-at i-vel kibővítve testet kapunk (amely kilenc elemű). Ugyanakkor $2^2+1^2 = 5$, vagyis ha $\mathbb{Z}_5$-ből indulunk ki, akkor $(2+i)(2-i) = 0$. Tehát a nullosztómentesség nem teljesül, és így nem kapunk testet.

2.2.20.

(1) Igen, mert $\varphi(x+y) = 2^{x+y} = 2^x 2^y = \varphi(x)\varphi(y)$.
(2) Igen, mert komplex számok szorzásakor a szögek összeadódnak: $\varphi(x+y) = \cos(x+y) + i\sin(x+y) = (\cos x + i\sin x)(\cos y + i\sin y) = \varphi(x)\varphi(y)$.
(3) Igen, $\varphi(x+y) = 60 *_{100} (x+y) = 60 *_{100} x + 60 *_{100} y = \varphi(x) + \varphi(y)$, mert a $\mathbb{Z}_{100}$ gyűrűben igaz a disztributivitás. (Mindegyik $+$ jel igazából $+_{100}$, csak az olvashatóság kedvéért lehagytuk ezeket az indexeket.)
(3) Vigyázzunk, ez formailag másik kérdés, mint az előző, mert a $60x$ úgy van definiálva, hogy az x-et összeadjuk önmagával 60 példányban. Ez a leképezés is művelettartó, mert igazából $60x = 60 *_{100} x$ teljesül. Ugyanis a $\mathbb{Z}_{100}$ gyűrűben igaz a disztributivitás, és ezért

$$60x = x + x + \cdots + x = (1 + 1 + \cdots + 1) *_{100} x = 60 *_{100} x\,.$$

Érdemes azonban meggondolni, hogy tetszőleges gyűrűben a $\varphi(x) = nx$ leképezés minden n egészre tartja az összeadást (a 2.2.8. Gyakorlat miatt).

2.2.21. Legyen a G_1 csoport egységeleme e_1, a G_2 csoport egységeleme e_2. Ekkor $e_1^2 = e_1$, és φ szorzattartása miatt

$$\varphi(e_1) = \varphi(e_1^2) = \varphi(e_1)^2\,.$$

Mindkét oldalt $\varphi(e_1)$ inverzével megszorozva (magyarán $\varphi(e_1)$-gyel egyszerűsítve) azt kapjuk, hogy $e_1 = \varphi(e_1)$.

Ha ezután $g \in G_1$ inverze h, akkor $gh = e_1$-re φ-t alkalmazva

$$\varphi(g)\varphi(h) = \varphi(gh) = \varphi(e_1) = e_2\,.$$

Ezért $\varphi(h)$ (a g inverzének a képe) tényleg g képének, azaz $\varphi(g)$-nek az inverze lesz. (Igazából balinverzre láttuk be az állítást. Ugyanígy beláthatjuk jobbinverzre, és ezáltal kétoldali inverzre is, vagy felhasználhatjuk, hogy csoportban a balinverz a 2.2.6. Feladat miatt kétoldali inverz is mindig.)

2.2.22. Bár a feladat szempontjából ez nem lényeges, a 2.2.15. Gyakorlat szerint itt tényleg két testről van szó. Legyen φ kölcsönösen egyértelmű művelettartó leképezés az első testből a másodikba. Az előző (2.2.21.) Feladatot az additív csoportra alkalmazva azt kapjuk, hogy $\varphi(0) = 0$. Mivel φ kölcsönösen egyértelmű, ebből következik, hogy a nem nulla elemek halmazát a nem nulla elemek halmazára képzi, és így használhatjuk ezt a feladatot még egyszer, most a multiplikatív csoportra. Az eredmény az, hogy $\varphi(1) = 1$. Ismét az előző feladat szerint φ az ellentettképzést is tartja, és így $\varphi(-1) = -1$ is teljesül. Ezután alkalmazzuk φ-t az $i^2 = -1$ összefüggésre. Azt kapjuk, hogy

$$-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2 .$$

Tehát az $u = \varphi(i)$ négyzete -1. De ilyen u nincs az $a + b\sqrt{2}$ alakú számok között, hiszen ezek valósak.

2.2.23. Az $(a_1 + \cdots + a_k) + (a_{k+1} + \cdots + a_n) = a_1 + \cdots + a_k$ képletet nyilván elfogadjuk. Ha $k = n-1$, akkor az $(a_1 + \cdots + a_{n-1}) + x = a_1 + \cdots + a_n$ összefüggésből nyilván $x = a_n$, vagyis az egytagú a_n összeget úgy érdemes értelmezni, hogy az egyetlen tagjával, a_n-nel egyenlő. Ha viszont $k = 0$, akkor az $(a_1 + \cdots + a_n) + x = a_1 + \cdots + a_n$ összefüggést kapjuk, ahol x most az üres összeg (egyáltalán nincs tagja). De ebből az egyenletből világos, hogy $x = 0$, vagyis az üres összeget nullának érdemes definiálni. Ha ugyanezt összeg helyett szorzással írjuk föl, akkor az derül ki, hogy az üres szorzat értékét 1-nek érdemes venni.

Az üres összeg és szorzat fogalma első ránézésre erőltetettnek tűnhet. Ugyanígy érezhettek az emberek akkor is, amikor először fogadták el a nullát számnak, vagy az üres halmazt halmaznak. Időről időre látni fogjuk, hogy az üres összeg és szorzat fogalma is rengeteg felesleges esetszétválasztást, extra megegyzést fog megspórolni.

2.3. A polinomok alaptulajdonságai.

2.3.1. Legyen

$$f(x) = \sum_{i=0}^{n} a_i x_i , \quad g(x) = \sum_{i=0}^{m} b_i x_i , \quad h(x) = \sum_{i=0}^{\ell} c_i x_i .$$

Az összeadás és a szorzás szabályai szerint x^k együtthatója $f(g + h)$-ban

$$\sum_{i+j=k} a_i (b_j + c_j)$$

$fg + fh$-ban pedig

$$\sum_{i+j=k} a_i b_j + a_i c_j .$$

Láthatjuk, hogy ez a két összeg egyenlő.

2.3.2.

(1) Nem alkotnak részgyűrűt, az összeadás kivezet, például $x^{20} + x$ és $-x^{20}$ is páros fokú, de az összegük x, ami páratlan fokú. (Azok a polinomok, amelyben minden nem nulla együtthatójú tag kitevője páros, részgyűrűt alkotnak, de az egy másik feladat.)

(2) Nem alkotnak részgyűrűt, az (1)-beli példa szerint az összeadás innen is kivezet.

2.3.3. Nem alkotnak gyűrűt. Az egyetlen tulajdonság, ami nem teljesül, a baloldali disztributivitás: $f \circ (g + h) = f \circ g + f \circ h$. Például ha $f(x) = x^2$, $g(x) = x$ és $h(x) = 1$, akkor x^2-be $x + 1$-et helyettesítve $(x + 1)^2$ adódik, ami nem egyenlő $x^2 + 1^2$-nel.

2.3.4. Jelölje $\overline{a}$ az $a \in \mathbb{Z}$ maradékát mod m. Legyen $f(x) = a_0 + a_1x + \cdots + a_nx^n$ és $h(x) = c_0 + c_1x + \cdots + c_mx^m$. Ekkor $\overline{f}\ \overline{h}$-ban az x^k-os tag együtthatója

$$\overline{a_0}\ \overline{c_k} + \cdots + \overline{a_k}\ \overline{c_0}\,,$$

az $\overline{fh}$-ban az x^k-os tag együtthatója pedig

$$\overline{a_0c_k + \cdots + a_kc_0}\,.$$

Ez a két együttható tényleg egyenlő, hiszen a felülvonás leképezés összeg- és szorzattartó (1.1.3. Állítás). Beláttuk tehát, hogy $\overline{f}\ \overline{h} = \overline{fh}$. Hasonlóan, de egyszerűbb számolással igazolható, hogy $\overline{f} + \overline{h} = \overline{f + h}$.

2.3.5. Ez az előző gyakorlat általánosítása, és a megoldás is ugyanúgy megy, csak $\overline{c}$ helyett mindenütt $\varphi(c)$-t kell írni.

2.4. Polinomfüggvények és gyökök.

2.4.1. Legyen $f(x) = a_0 + a_1x + \cdots + a_nx^n$ és $g(x) = c_0 + c_1x + \cdots + c_nx^n$. Ekkor

$$(f + g)^*(b) = (a_0 + c_0) + (a_1 + c_1)b + \cdots + (a_n + c_n)b^n\,,$$

és

$$f^*(b) + g^*(b) = (a_0 + a_1b + \cdots + a_nb^n) + (c_0 + c_1b + \cdots + c_nb^n)\,.$$

Ez a két összeg nyilván egyenlő. Hasonlóan, bár picit bonyolultabb számolással igazolható az $(fg)^*(b) = f^*(b)g^*(b)$ összefüggés is.

2.4.2. Jelölje B a Horner-elrendezés utolsó cellájában szereplő $bc_0 + a_0$ értéket (amiről meg kell mutatnunk, hogy $f^*(b)$-vel egyenlő). Beszorzással, és x szerint rendezve:

$$(x - b)(c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_jx^j + \cdots + c_1x + c_0) + B =$$
$$= c_{n-1}x^n + \cdots + (c_{j-1} - bc_j)x^j + \cdots + (c_0 - bc_1)x - bc_0 + B\,.$$

A Horner-elrendezés táblázatából tudjuk, hogy $c_{n-1} = a_n$, továbbá $c_{j-1} - bc_j = a_j$ (ha $1 \le j < n$), és végül $-bc_0 + B = a_0$. Tehát tényleg az eredeti f polinomot kapjuk. A b-t behelyettesítve pedig $f^*(b) = B$ adódik (hiszen $x - b$ nullává válik).

2.4.3. Mivel egy gyöktényező főegyütthatója 1, ami soha nem lehet nullosztó, gyöktényezővel való szorzáskor a fokszám mindig eggyel nő. Tehát az igaz nullosztómentesség nélkül is, hogy ha $f(x) = (x-b_1)\dots(x-b_k)q(x)$, akkor $k \le \mathrm{gr}(f)$. Csak az nem biztos, hogy minden gyök szerepel az itt felsoroltak között (amire mutattunk is példát).

2.4.4.

(1) Ezekből (egyszerre) kiemelhető az $n-1$ darab $(x-a_i)$ gyöktényező mindegyike, ahol $i \neq j$. Mivel a polinom $n-1$-edfokú, már csak egy konstans maradhat.

(2) Az a_j-t behelyettesítve e konstans értékét meghatározhatjuk. Az eredmény:

$$f_j(x) = \frac{(x-a_1)\dots(x-a_{j-1})(x-a_{j+1})\dots(x-a_n)}{(a_j-a_1)\dots(a_j-a_{j-1})(a_j-a_{j+1})\dots(a_j-a_n)}\,.$$

Ezek a *Lagrange-féle alappolinomok*.

(3) $f(x) = b_1 f_1(x) + \dots + b_n f_n(x)$ jó lesz. Ha ugyanis a_j-t behelyettesítjük, akkor egy kivétellel az összeg mindegyik tagja nullává válik (hiszen $f_i(a_j) = 0$ ha $i \neq j$), a megmaradó tag pedig $b_j f_j(a_j) = b_j$ lesz, hiszen $f_j(a_j) = 1$.

2.4.5.

(1) Mivel $(f+g)(a_j) = b_j = f(a_j)$, ezért a g polinomnak gyöke az $a_1, a_2, \dots a_{n-1}$. De g foka $n-1$, ezért

$$g(x) = c(x-a_1)\dots(x-a_{n-1})$$

alkalmas c konstansra.

(2) A b_n-et behelyettesítve

$$c = \frac{b_n - f(a_n)}{(a_n-a_1)\dots(a_n-a_{n-1})}$$

adódik.

2.4.6. A Horner-elrendezés táblázata a következő lesz:

	1	0	−4	1	−1	0	4
2	1	2	0	1	1	2	$\boxed{8}$

Ezért a 2 nem gyöke f-nek, és $f(x) = (x-2)(x^5+2x^4+x^2+x+2)+8$.

2.4.7. Ha $f(x) = a_n x^n + \dots + a_0$, akkor

$$f(x) - f^*(b) = \sum_{j=0}^{n} a_j (x^j - b^j)\,.$$

A zárójelben álló kifejezések mindegyikéből kiemelhető $(x-b)$, és ami marad, az x-nek egy polinomja lesz.

2.4.8. Akkor és csak akkor, ha m összetett szám. Ha ugyanis $m = ab$, ahol $1 < a, b < m$, akkor az ax elsőfokú polinomnak (legalább) két gyöke van: a 0 és a b. Ha viszont m prímszám, akkor $\mathbb{Z}_m$ nullosztómentes (2.2.15. Állítás), és így a 2.4.5. Tétel miatt minden polinomnak legfeljebb annyi gyöke van, mint a foka.

2.4.9. Legyenek a test elemei $a_1, \ldots, a_n$. Ekkor az

$$(x - a_1) \ldots (x - a_n) + 1$$

polinomnak nyilván nincs gyöke ebben a testben. (Az 1 a test egységeleme, de bármelyik nem nulla elemet írhatnánk a helyére.)

2.4.10. Az eredmény $(1/2)x^3 - (3/2)x^2 + x + 3$ (például Newton-interpolációval).

2.4.11. Legyen f egy n-edfokú polinom, amely minden racionális helyen racionális értéket vesz föl. Válasszunk ki $n + 1$ racionális helyet bárhogy, például az $1, 2, \ldots, n + 1$ helyeket, és készítsük el azt a g interpolációs polinomot, amely ezeken a helyeken ugyanazt az értéket veszi föl, mint az f. Persze a g racionális együtthatós (ez például a Lagrange-interpolációnál használt képletekből látszik, de elegánsabban azt mondhatnánk, hogy mivel $\mathbb{Q}$ test, ezért $\mathbb{Q}$ fölött elvégezhető az interpoláció, és az eredmény persze $\mathbb{Q}[x]$-beli.) Ekkor f és g két legfeljebb n-edfokú polinom, amelyek $n + 1$ helyen megegyeznek. A polinomok azonossági tételét (2.4.6. Következmény) a komplex test fölött alkalmazva azt kapjuk, hogy $f = g$, tehát g is racionális együtthatós.

A második állítás nem igaz, például $x(x + 1)/2$ nem egész együtthatós, de egész helyen egész értéket vesz föl, hiszen két szomszédos egész szám közül az egyik mindig páros. Tetszőleges k-ra van ilyen k-adfokú polinom is, például az

$$\frac{x(x - 1) \ldots (x - k + 1)}{k!}$$

„binomiális együttható”.

2.4.12. Mivel $f(14) = 440$, az f-et kereshetjük $(x - 14)g(x) + 440$ alakban, ahol g is egész együtthatós polinom. A másik két feltételt behelyettesítve átrendezéssel $g(10) = 10$ és $g(18) = 20$ adódik. Innen akár az $a - b \mid g(a) - g(b)$ összefüggést felhasználva (2.4.7. Gyakorlat), akár g-t $(x - 10)h(x) + 10$ alakban felírva a $8 \mid 10$ ellentmondás adódik. Ilyen polinom tehát nem létezik. Megjegyezzük, hogy a következő feladat állítása segítségével is megmutatható, hogy nincs ilyen polinom.

2.4.13. Legyen f egész együtthatós polinom, amelyre $f(a_i) = b_i$, ha $1 \leq i \leq n$, ahol az a_i számok páronként különböző egészek (és így b_i is egész). Jelölje f_k azt az (egyértelműen meghatározott) legfeljebb $k-1$-edfokú polinomot, amely f-et az $a_1, \ldots, a_k$ helyeken interpolálja. Azt kell megmutatnunk, hogy f_n egész együtthatós. Ehhez k szerinti indukcióval belátjuk, hogy f_k egész együtthatós.

Ha $k = 1$, akkor f_1 a konstans b_1 polinom, ami tényleg egész együtthatós. Tegyük fel, hogy f_{k-1} egész együtthatós, be kell látnunk, hogy f_k is az. Az interpolációs polinom

egyértelműsége miatt f_k-t felírhatjuk a Newton-interpoláció segítségével is:

$$f_k(x) = (x - a_1) \dots (x - a_{k-1})c + f_{k-1}(x)\,,$$

ahol a c számot az a_k behelyettesítésével kapjuk meg:

$$b_k = f(a_k) = f_k(a_k) = (a_k - a_1) \dots (a_k - a_{k-1})c + f_{k-1}(a_k)\,.$$

Ha meg tudnánk mutatni, hogy ebből az egyenletből c-re egész szám adódik, akkor készen lennénk. Azonban

$$f(x) - f_{k-1}(x) = (x - a_1) \dots (x - a_{k-1})h(x)\,,$$

ahol h egész együtthatós polinom, hiszen $f(a_i) = b_i = f_{k-1}(a_i)$ ha $i < k$, és így a_i gyöke $f(x) - f_{k-1}(x)$-nek. Ebbe az egyenlőségbe x helyére a_k-t helyettesítve látjuk, hogy az (egész) $c = h(a_k)$ érték megfelel a kívánalmaknak.

2.4.14. Legyen $r \neq 0$ eleme R-nek. Ha $f \in R[x]$ olyan, hogy $f(0) = 0$ és $f(r) = 1$, akkor az $f(x)$-ből az $x - 0$ gyöktényezőt kiemelve $f(x) = xg(x)$ adódik. Ide r-et helyettesítve azt kapjuk, hogy $1 = rg(r)$, azaz $g(r)$ inverze r-nek.

2.4.15. Az, hogy az $R \to R$ függvények kommutatív gyűrűt alkotnak a pontonkénti összeadásra és a szorzásra, könnyen ellenőrizhető (és később lesz róla szó, amikor a gyűrűk direkt szorzatát tárgyaljuk). Az azonosságok azért teljesülnek, mert minden egyes r behelyettesítésekor teljesülnek a kapott értékekre. Például az $f(g + h) = fg + fh$ disztributív szabály igazolásához azt kell megmutatni, hogy e két függvény minden $r \in R$ helyen megegyezik. A pontonkénti összeadás és szorzás definíciója miatt ez azt jelenti, hogy

$$f(r)\big(g(r) + h(r)\big) = f(r)g(r) + f(r)h(r)\,,$$

ami valóban teljesül, hiszen R gyűrű. A nullelem a konstans nulla függvény, az ellentett pedig a *pontonkénti ellentett:*

$$(-f)(r) = -f(r)\,.$$

Az egységelem a konstans 1 függvény lesz.

Az R azért nem nullosztómentes, mert ha a (legalább kételemű) alaphalmazát két részre osztjuk, az f függvény az első részen nulla, és a másikon nem, a g függvény pedig a másik részen nulla, és az elsőn nem, akkor fg már azonosan nulla lesz. Az (1) állítás tehát igaz.

A 2.4.1. Gyakorlat szerint

$$(f + g)^*(b) = f^*(b) + g^*(b) \qquad \text{és} \qquad (fg)^*(b) = f^*(b)g^*(b)\,,$$

ami maga a (3) állítás. De ez azt is jelenti, hogy

$$(f + g)^* = f^* + g^* \qquad \text{és} \qquad (fg)^* = f^*g^*\,,$$

ahol a két egyenlőség baloldalán polinom-műveletek, a jobboldalukon pontonkénti műveletek állnak. Így az $f \mapsto f^*$ leképezés összeg- és szorzattartó (ami a (4) állítás). Innen az is látszik, hogy a polinomfüggvények halmaza zárt a pontonkénti műveletekre. Nyilván

a nullapolinomhoz az azonosan nulla függvény, a konstans 1 polinomhoz pedig az azonosan 1 függvény tartozik, és a $(-f)^*$ az f^* pontonkénti ellentettje. Így a polinomfüggvények részgyűrűt alkotnak az $R \to R$ függvények gyűrűjében, amely az egységelemet is tartalmazza, és ezzel a (2) állítást is beláttuk.

2.4.16. Álljon S azokból a függvényekből, melyeknek a 2 szám gyöke. Ez a 2.2.10. Feladatbeli tulajdonságok (azaz az összeadásra, szorzásra és ellentettképzésre való zártság) ellenőrzésével könnyen láthatóan részgyűrű. E részgyűrű egységeleme az a függvény, amely a 2 helyen nullát, a többi helyen 1-et vesz föl. Ezzel szemben R egységeleme a konstans 1 függvény.

Legyen most R nullosztómentes gyűrű, melynek egységelemét e jelöli, és S egységelemes részgyűrű, melynek egységeleme legyen f. Mivel az egységelemes gyűrűk közül kizártuk a nullgyűrűt, $f \neq 0$. Nyilván $ff = f = fe$ (az első egyenlőség azért igaz, mert f egységelem S-ben, a második pedig azért, mert e egységelem R-ben). Az egyszerűsítési szabály (2.2.11. Gyakorlat) miatt innen $e = f$.

2.5. A gyöktényezős alak.

2.5.1. Mivel szorzáskor a fokszámok összeadódnak, egy konstans foka nulla, egy gyöktényező foka pedig 1, ezért a gyöktényezők száma tényleg a polinom foka lesz (ezt a gondolatmenetet már használtuk a 2.4.5. Tételben, lásd a 2.4.3. Gyakorlat megoldását is).

A c konstans kiszámításához használjuk föl, hogy polinomok szorzatának főtagja a főtagok szorzata. Így a gyöktényezős alakot beszorozva a főtag $c \cdot x \cdot x \cdot \ldots \cdot x = cx^n$ lesz. Vagyis c tényleg a főegyüttható.

2.5.2. Legyen $r \neq 0$ eleme R-nek. Ekkor az $rx - 1$ polinom elsőfokú, és ezért van gyöke, ami nyilván r inverze lesz. Tehát minden nem nulla elem invertálható.

2.5.3. Tegyük fel, hogy $(x - b)^k g(x) = (x - b)^m h(x)$, ahol sem $g(b)$, sem $h(b)$ nem nulla. Mivel az $x - b$ nem a nullapolinom, egyszerűsíthetünk vele a 2.2.9. Feladat szerint. Ha $k < m$, akkor tehát $g(b) = (x - b)^{m-k} h(x)$ marad, ami nem lehet, mert g-nek b nem gyöke. Ugyanígy zárható ki a $k > m$ lehetőség is. Tehát $k = m$, azaz k egyértelműen meghatározott.

Ha ezután f-et kanonikus alakban írjuk fel:

$$f(x) = c(x - d_1)^{k_1}(x - d_2)^{k_2} \ldots (x - d_m)^{k_m},$$

akkor a d_j tényleg k_j-szoros gyök lesz az új értelemben is, hiszen $(x - d_j)^{k_j}$ kiemelhető, a megmaradó polinomnak pedig a d_j már nem gyöke (a nullosztómentesség miatt).

2.5.4. Az $(x-b_1)(x-b_2)(x-b_3)$ beszorozva és rendezve az

$$x^3-(b_1+b_2+b_3)x^2+(b_1b_2+b_1b_3+b_2b_3)x-b_1b_2b_3$$

alakot ölti. Az $(x-b_1)(x-b_2)(x-b_3)(x-b_4)$ beszorzását a 2.1.4. Gyakorlat felhasználásával végezzük el. Mindegyik zárójelből egy tagot kell választanunk, ezeket összeszorozni, és a kapott szorzatokat összeadni. Rögtön rendezünk is x hatványai szerint.

Az x^4 csak úgy keletkezhet, ha mindegyik zárójelből x-et választunk. Egy ilyen tag van, amelynek tehát az együtthatója 1. Az x^3 akkor keletkezik, ha három zárójelből választunk x-et, a negyedikből tehát $-b_j$-t kell választanunk. Ez négyféleképpen lehetséges, és így x^3 együtthatója

$$-(b_1+b_2+b_3+b_4)\,.$$

Az x^2 úgy keletkezhet, hogy két zárójelből x-et, a másik kettőből $-b_j$-t választunk. Négy zárójelből kettőt hatféleképpen lehet kiválasztani, tehát hat ilyen tag lesz. Az x^2 együtthatója tehát

$$b_1b_2+b_1b_3+b_1b_4+b_2b_3+b_2b_4+b_3b_4$$

(az előjel persze $+$, hiszen $(-b_i)(-b_j)=b_ib_j$). Az x úgy keletkezik, hogy három zárójelből választunk $-b_j$-t, tehát x együtthatója

$$b_1b_2b_3+b_1b_2b_4+b_1b_3b_4+b_2b_3b_4\,.$$

Végül a konstans tag esetében mindegyik zárójelből a $-b_j$-t választjuk, tehát ez $b_1b_2b_3b_4$.

2.5.5. Az $x^4=4$ egyenlet gyökei a -4 szám negyedik gyökei. Ezeket már meghatároztuk az 1.5.5 (2) (sőt az 1.2.9.) Gyakorlatban, az eredmény $\pm1\pm i$ lett. Mivel x^4+4 főegyütthatója 1, a gyöktényezős alak a következő:

$$x^4+4=1\cdot\big(x-(1+i)\big)\big(x-(1-i)\big)\big(x-(-1+i)\big)\big(x-(-1-i)\big)\,.$$

A beszorzást ügyesen elvégezhetjük, ha felhasználjuk az $(a-b)(a+b)=a^2-b^2$ azonosságot. Az első két tényező szorzata ugyanis

$$(x-1-i)(x-1+i)=(x-1)^2-i^2=x^2-2x+2\,.$$

Ugyanígy kapjuk, hogy a második két tényező szorzata x^2+2x+2. Tehát

$$x^4+4=(x^2-2x+2)(x^2+2x+2)$$

valós (sőt egész) együtthatós polinomok szorzatára való felbontás. (Az, hogy az i kiesett, azon múlt, hogy ügyesen párosítottuk a gyöktényezőket: minden gyököt a konjugáltjával.) Folytassuk most a beszorzást, újra felhasználva az $(a-b)(a+b)=a^2-b^2$ azonosságot:

$$(x^2-2x+2)(x^2+2x+2)=(x^2+2)^2-(2x)^2=x^4+4\,.$$

Tehát tényleg visszakaptuk az eredeti polinomot.

2.5.6. Az $x-1$ gyöktényező kiemelése után maradó polinom a Horner-elrendezés alsó sorában található. Erre ismét a Horner-elrendezést kell alkalmaznunk, és ezt addig folytatjuk, amíg az 1 már nem lesz gyök. Ezért a legegyszerűbb egy táblázatot készíteni több sorral:

	1	−1	0	−1	1
1	1	0	0	−1	**0**
1	1	1	1	**0**	
1	1	2	**3**		

$$x^4-x^3-x+1 = (x-1)(x^3-1) = (x-1)^2(x^2+x+1)\,.$$

Mivel a táblázat utolsó sora szerint x^2+x+1-nek az 1 már nem gyöke, ezért az eredeti polinomnak az 1 pontosan kétszeres gyöke.

2.5.7. A polinomok azonossági tételének (2.4.6. Következmény) a bizonyítását módosítjuk. Legyen f és g a két polinom. Ekkor $f-g$-ből kiesik a főtag, és ezért ez a különbség legfeljebb $n-1$-edfokú. De legalább n gyöke van, és így csak a nullapolinom lehet.

2.5.8. Emeljük négyzetre a $\sigma_1 = x_1+\cdots+x_n$ összeget. Ekkor (a 2.1.2. Gyakorlat szerint) egy olyan összeget kapunk, amelynek tagjai az összes lehetséges x_ix_j szorzatok. Ha $i=j$, akkor ez x_i^2, ezek együtt a keresett négyzetösszeget adják. Ha $i\neq j$, akkor viszont x_ix_j és x_jx_i is szerepel, tehát az ilyen tagokból σ_2 kétszeresét kapjuk. Így végülis

$$x_1^2+\cdots+x_n^2 = \sigma_1^2-2\sigma_2 \quad (\text{ha } n\geq 2).$$

Ezt az összefüggést általánosítjuk majd a 2.7.4. Tételben.

2.5.9. Alkalmazzuk a gyökök és együtthatók összefüggését (2.5.5. Következmény). Ha

$$f(x) = 2x^4+2x+3 = a_4x^4+a_3x^3+a_2x^2+a_1x+a_0\,,$$

akkor $a_4=2$, $a_3=a_2=0$, $a_1=2$ és $a_0=3$. Ezért

$$\sigma_1 = b_1+b_2+b_3+b_4 = (-1)^1a_3/a_4 = 0\,,$$
$$\sigma_2 = b_1b_2+b_1b_3+b_1b_4+b_2b_3+b_2b_4+b_3b_4 = (-1)^2a_2/a_4 = 0\,,$$
$$\sigma_3 = b_1b_2b_3+b_1b_2b_4+b_1b_3b_4+b_2b_3b_4 = (-1)^3a_1/a_4 = -1\,,$$
$$\sigma_4 = b_1b_2b_3b_4 = (-1)^4a_0/a_4 = 3/2\,.$$

Tehát a gyökök összege nulla, szorzata $3/2$ négyzetösszege az előző (2.5.8.) Gyakorlat szerint $\sigma_1^2-2\sigma_2=0$, végül a gyökök reciprokainak összege

$$\frac{1}{b_1}+\frac{1}{b_2}+\frac{1}{b_3}+\frac{1}{b_4} = \frac{b_1b_2b_3+b_1b_2b_4+b_1b_3b_4+b_2b_3b_4}{b_1b_2b_3b_4} = \frac{\sigma_3}{\sigma_4} = -\frac{2}{3}\,.$$

Megjegyezzük, hogy fel tudunk írni közvetlenül is egy olyan polinomot, aminek a gyökei az f polinom gyökeinek reciprokai, ez

$$g(x) = x^4f(1/x) = 3x^4+2x^3+2$$

lesz. A $f(x)$ polinom gyökei reciprokainak összegét tehát a $g(x)$ polinomból mint a gyökök összegét olvashatjuk le.

2.5.10. Az $x^n - 1$ polinom főegyütthatója 1, gyökei pontosan az n-edik egységgyökök, és ezért valóban

$$x^n - 1 = (x - \varepsilon_1) \dots (x - \varepsilon_n) .$$

Speciálisan $x^4 - 1 = (x - 1)(x - i)(x + 1)(x + i)$.

Az n-edik egységgyökök összegét, szorzatát és négyzetösszegét már meghatároztuk az 1.5.13. Gyakorlatban, a mostani eszköztárunk azonban gyorsabb megoldást kínál. Az $\varepsilon_1 \dots \varepsilon_n$ szorzatot a gyökök és együtthatók összefüggése (a 2.5.5. Következmény) felhasználásával megkaphatjuk az $x^n - 1$ polinomból. Ennek a polinomnak a konstans tagja $a_0 = -1$, főegyütthatója $a_n = 1$, és így

$$\varepsilon_1 \dots \varepsilon_n = \sigma_n(\varepsilon_1, \dots \varepsilon_n) = (-1)^n a_0/a_n = (-1)^n \cdot (-1)/1 = (-1)^{n+1}$$

(sőt ez a 0 behelyettesítésével is azonnal adódik). Ugyanígy olvasható le az $\varepsilon_1 + \dots + \varepsilon_n$ összeg az $x^n - 1$ polinomban az x^{n-1}-es tag a_{n-1} együtthatójáról:

$$\varepsilon_1 + \dots + \varepsilon_n = \sigma_1(\varepsilon_1, \dots \varepsilon_n) = (-1)^1 a_{n-1}/a_n .$$

De $a_{n-1} = 0$ ha $n \geq 2$ (és így az n-edik egységgyökök összege is nulla ilyenkor), ha viszont $n = 1$, akkor ez az együttható -1, és ekkor eredményül $(-1)^1(-1) = 1$ adódik. Végül a gyökök négyzetösszegének kiszámításához a 2.5.8. Gyakorlatot használjuk fel. Az $x^n - 1$ polinomban az x^{n-2}-es tag a_{n-2} együtthatója nulla ha $n > 2$, ezért $\sigma_2(\varepsilon_1, \dots \varepsilon_n)$ is nulla, és így

$$\varepsilon_1^2 + \dots + \varepsilon_n^2 = \sigma_1^2 - 2\sigma_2 = 0 .$$

Ha $n = 2$, akkor az eredmény 2 lesz (ami közvetlenül is világos: $1^2 + (-1)^2 = 2$). Végül $n = 1$-re a négyzetösszeg $1^2 = 1$ (ekkor már a σ_2 nincs is értelmezve).

Végül (4) igazolásához helyezzük el a sokszöget úgy, hogy csúcsai pont az n-edik egységgyökök legyenek, és az $\varepsilon_n = 1$-hez tartozó csúcsból húzzuk meg az átlókat. Mivel két pont távolsága a különbségük abszolút értéke (1.4.3. Gyakorlat), és $\varepsilon_n = 1$, ezért az

$$|(1 - \varepsilon_1)| \cdot \dots \cdot |(1 - \varepsilon_{n-1})|$$

szorzatot kell kiszámítani. Az ismert azonosság (a mértani sor összegképlete) szerint

$$x^n - 1 = (x - 1)(x^{n-1} + \dots + x + 1)$$

Ezt vessük össze az $x^n - 1$ gyöktényezős alakjával, és egyszerűsítsünk az $x - 1$ polinommal (ezt szabad a 2.2.9. Feladat szerint, hiszen $x - 1$ nem a nullapolinom). Azt kapjuk, hogy

$$(x - \varepsilon_1) \dots (x - \varepsilon_{n-1}) = x^{n-1} + \dots + x + 1 .$$

Az x helyébe 1-et helyettesítve, és mindkét oldal abszolút értékét véve az állítást kapjuk (hiszen az abszolút érték szorzattartó).

Nem osztottunk ebben a bizonyításban nullával? Hiszen $x-1$-gyel egyszerűsítettünk, és ezután x helyére 1-et írtunk. Több ismert tréfás gondolatmenetben hasonló trükkel ellentmondást lehet kihozni!

A válasz az, hogy az $x-1$ *polinommal* egyszerűsítettünk, ami nem a nullapolinom, vagyis $\mathbb{C}[x]$ nullosztómentességét használtuk fel. De érdemes máshogy is meggondolni ezt a problémát. A fenti gondolatmenet mintája az, hogy az

$$f(x)(x-1) = g(x)(x-1)$$

polinomegyenlőségből következtettünk arra, hogy $f(1) = g(1)$. Ha polinomfüggvényekkel akarunk számolni, akkor annyi biztosan igaz, hogy $f^*(b) = g^*(b)$ minden $b \neq 1$-re. Az f és g polinomokhoz tartozó polinomfüggvények tehát végtelen sok helyen megegyeznek (minden $b \neq 1$ komplex számra), és így az f és g polinomok az azonossági tétel miatt egyenlők (együtthatóról együtthatóra), vagyis már a $b = 1$ helyen is egyenlők.

Ez a gondolatmenet komplex felett működik, de véges testek fölött nem biztos, mert annak a testnek esetleg kevesebb eleme van, mint a szereplő polinomok foka. Az első gondolatmenetünk, amikor $x-1$-gyel egyszerűsítettünk, ennyiben jobb: az minden test fölött működik.

2.5.11. Nem. A legegyszerűbb ellenpélda az, hogy a $\mathbb{Z}_2$ test fölött az x^k polinomokhoz $k \geq 1$ esetén ugyanaz a polinomfüggvény tartozik: az identikus leképezés. Ezen polinomok esetében a 0 gyök multiplicitása más és más. Tehát a polinomfüggvény nem határozza meg a gyökök multiplicitását (hanem csak a gyökök halmazát).

2.6. Többhatározatlanú polinomok.

2.6.1. A 2.1.2. Gyakorlat szerint szorozzuk össze az f és g polinomokat, azaz minden tagot minden taggal. Ha f egy i-edfokú P tagját g egy j-edfokú Q tagjával szorozzuk, akkor a PQ eredmény nyilván $i+j$-ed fokú lesz. Azokat a PQ tagokat keressük, amikor $i+j=k$, tehát $j=k-i$. Az i-edfokú P tagok az f_i-ben vannak összegyűjtve, ezeket tehát a g polinom $k-i$-edfokú tagjaival, azaz g_{k-i}-vel kell megszorozni, hogy k-adfokú tagokat kapjunk.

Legyen f foka n, és g foka m. Ekkor az előzőek szerint fg-ben nincsen $m+n$-nél magasabb fokú tag, az $m+n$-edfokú tagok pedig az $f_n g_m$ szorzat tagjai. Azt kell tehát megmutatni, hogy $f_n g_m \neq 0$. Ez azonban világos, hiszen a 2.6.2. Állítás szerint a többhatározatlanú polinomok szorzása nullosztómentes.

2.6.2. Először egy konkrét példát mutatunk.

$$f(x_1, x_2, x_3) = x_1x_2^4 - x_1x_2x_3 - 3x_2^3 + x_3^2 + 2x_1^2 + x_1x_2x_3^3\,.$$

Első lépésben x_1 szerint rendezünk:

$$(-3x_2^3 + x_3^2) + (x_2^4 - x_2x_3 + x_2x_3^3)x_1 + 2x_1^2\,,$$

majd a zárójeleken belül x_2 szerint:

$$(x_3^2 - 3x_2^3) + \big((-x_3 + x_3^3)x_2 + 1\cdot x_2^4\big)x_1 + 2x_1^2\,,$$

és a legbelső zárójelben már x_3 szerint is rendezve van a polinom. Beszorozva, de a sorrendet nem megváltoztatva a következőt kapjuk:

$$x_3^2 - 3x_2^3 - x_1x_2x_3 + x_1x_2x_3^3 + x_1x_2^4 + 2x_1^2 .$$

Ez pedig tényleg a lexikografikusan növekvő sorrend.

Az alábbi általános gondolatmenetet a fenti példán érdemes nyomon követni. Tegyük fel, hogy az eredeti polinomnak tagja $P = rx_1^{m_1} \dots x_n^{m_n}$ és $Q = sx_1^{k_1} \dots x_n^{k_n}$, és ezek közül az első a lexikografikusan kisebb, azaz van olyan j index, hogy $m_i = k_i$ minden $i < j$ esetén, de $m_j < k_j$. (Gondoljunk a fenti példában az $x_1x_2x_3^3$ és az $x_1x_2^4$ tagokra.) Amikor a polinomot először x_1 hatványai szerint rendezzük, akkor mind P-ből, mind Q-ból $x_1^{m_1}$-et emelünk ki, és ami megmarad, az az $x_1^{m_1}$ együtthatójában fog szerepelni (a fenti példában ez az együttható $x_2^4 - x_2x_3 + x_2x_3^3$). Mostantól kezdve már csak ezt az együtthatót vizsgáljuk, és x_2 hatványai szerint rendezzük. Egészen addig „együtt marad" P és Q, amíg el nem érünk az x_j szerinti rendezéshez (a fenti példában $j = 2$). Ennél a lépésnél a P-nek megfelelő tag az $x_j^{m_j}$ együtthatójába kerül (jelölje ezt az együtthatót p, a fenti példában $m_j = 1$, $p = -x_3 + x_3^3$, ebben a P-nek megfelelő tag x_3^3, hiszen $P = x_1x_2x_3^3$), a Q-nak megfelelő tag pedig az $x_j^{k_j}$ együtthatójába (jelölje ezt q, a fenti példában $k_j = 4$, $q = 1$, hiszen $Q = x_1x_2^4 \cdot 1$). Mivel $m_j < k_j$, a p együtthatót írjuk le „előbb", vagyis a q-hoz képest a „baloldalra". Amikor a még magasabb indexű változók szerint rendezünk (a fenti példában az x_3 szerint), akkor már a p és q együtthatókon belül cserélgetünk csak, tehát P és Q sorrendje már nem változik meg.

2.6.3. A homogén komponensek a következők:

$$\begin{aligned} p_5 &= ix_1x_2x_3x_4^2 - x_1^2x_3^3 + 2x_1^2x_2x_3x_4 - 6x_1^2x_2^2x_4 - x_1^2x_2^2x_3 + \pi x_1^2x_2^3 \\ p_4 &= 3x_1^3x_2 \\ p_1 &= x_4 , \end{aligned}$$

itt p_5 tagjai már lexikografikusan növő sorrendben vannak felírva. A p polinom főtagja $3x_1^3x_2$, ezért p^7 főtagja $3^7x_1^{21}x_2^7$. Viszont p^7 foka $7 \cdot 5 = 35$, és így a legnagyobb fokú tagok között a lexikografikusan legnagyobb a 2.6.1. Gyakorlat szerint $(\pi x_1^2x_2^3)^7 = \pi^7x_1^{14}x_2^{21}$ lesz.

2.6.4. Legyen $f \in R[x_1, \dots, x_n]$. Ebbe a polinomba n darab R-beli elemet akarunk behelyettesíteni: x_i helyére b_i-t, ahol $1 \le i \le n$. Ezt röviden úgy fogjuk mondani, hogy az f polinomba a $\mathbf{b} = (b_1, \dots, b_n)$-et helyettesítjük be, ezeknek az R-beli elem-n-eseknek a halmazát R^n jelöli majd, és b_i-t a $\mathbf{b}$ „pont" i-edik *koordinátájának* nevezzük (az elnevezés és a szemlélet persze a geometriából származik).

Az $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$ definíció szerint tetszőleges n-határozatlanú polinom

$$f = g_0 + g_1x_n + \dots + g_kx_n^k$$

alakban írható, ahol $g_0, \ldots, g_k \in R[x_1, \ldots, x_{n-1}]$. Az $f(b_1, \ldots, b_n)$ értékét tehát n szerinti indukcióval definiálhatjuk, azaz feltehetjük, hogy $n-1$-változós polinomba már be tudunk helyettesíteni. Eszerint az $a_i = g_i(b_1, \ldots, b_{n-1})$ már ismert. Legyen

$$f(\mathbf{b}) = a_0 + a_1 b_n + \cdots + a_k b_n^k .$$

Az olvasót arra biztatjuk, hogy a pontonkénti műveletek 2.4.2. Definícióját általánosítsa többváltozós függvényekre is, és vizsgálja meg, hogy a 2.4.15. Gyakorlat állításai érvényben maradnak-e többváltozós polinomokra.

2.6.5. Legyen T test, az előző gyakorlatban bevezetett jelöléseket használjuk. Adottak tehát az $\mathbf{a}^1, \ldots, \mathbf{a}^k \in T^n$ páronként különböző „pontok", és a $b_1, \ldots, b_k$ értékek. Olyan $f \in T[x_1, \ldots, x_n]$ polinomot keresünk, amelyre $f(\mathbf{a}^i) = b_i$, ha $1 \le i \le k$.

A Newton-interpolációt modellezzük, azaz k szerinti indukciót alkalmazunk. Egy pont esetében nyilván jól interpolál egy konstans polinom. Tegyük fel, hogy van olyan f, ami már az első $k-1$ helyen a megadott értéket veszi föl. Ha találunk olyan g polinomot, amelyre $g(\mathbf{a}^i) = 0$, ha $1 \le i \le k-1$, de $g(\mathbf{a}^k) \neq 0$ akkor az $f + cg$ nyilván megoldása a feladatnak, ahol $c = b_k / g(\mathbf{a}^k)$.

Mivel az alappontok különbözők, az $\mathbf{a}^k = (a_1^k, \ldots, a_n^k)$ és $\mathbf{a}^i = (a_1^i, \ldots, a_n^i)$ sem egyenlő, azaz valamelyik koordinátájuk különbözik. Jelölje a megfelelő indexet $u(i)$, tehát akkor tudjuk, hogy $a^i_{u(i)} \neq a^k_{u(i)}$. Behelyettesítéssel azonnal láthatjuk, hogy

$$g(x_1, \ldots, x_n) = (x_{u(1)} - a^1_{u(1)}) \ldots (x_{u(k-1)} - a^{k-1}_{u(k-1)})$$

megfelel a kívánalmaknak.

2.7. Szimmetrikus polinomok.

2.7.1. A σ_k főtagja $x_1 \ldots x_k$ (hiszen azok között az n jegyű „telefonszámok" között, amelyekben k darab 1-es van, és a többi számjegy nulla, nyilván az a legnagyobb, ahol az 1-es számjegyek a legnagyobb helyiértékeket foglalják el). Mivel szorzat főtagja a főtagok szorzata, ezért $r\sigma_1^{k_1}\sigma_2^{k_2} \ldots \sigma_n^{k_n}$ főtagja

$$r(x_1 x_2 \ldots x_n)^{k_1}(x_2 \ldots x_n)^{k_2} \ldots (x_{n-1}x_n)^{k_{n-1}} x_n^{k_n} = r x_1^{k_1+\cdots+k_n} x_2^{k_2+\cdots+k_n} \ldots x_{n-1}^{k_{n-1}+k_n} x_n^{k_n} .$$

2.7.2. Tegyük fel, hogy $m_1 \ge m_2 \ge \cdots \ge m_n$ nem igaz, hanem mondjuk $m_j < m_{j+1}$ teljesül valamelyik j indexre. Cseréljük meg a főtagban az x_j és az x_{j+1} változókat. Mivel a polinom szimmetrikus, a kapott

$$r x_1^{m_1} x_2^{m_2} \ldots x_{j-1}^{m_{j-1}} x_j^{m_{j+1}} x_{j+1}^{m_j} x_{j+2}^{m_{j+2}} \ldots x_n^{m_n}$$

is tagja a polinomunknak, de ez lexikografikusan nagyobb a főtagnál, ami ellentmondás. Ezért a főtag kitevői tényleg egyre kisebbednek.

Ha a polinom valamelyik tagjában szerepelne egy $x_j^{k_j}$, ahol $k_j > m_1$, akkor az x_1 és x_j cseréjével olyan tagot kapnánk, amelyben az x_1 kitevője nagyobb m_1-nél. De ez lehetetlen, mert akkor ez a tag lexikografikusan nagyobb lenne a főtagnál.

Ezek szerint valamennyi tagban valamennyi határozatlan kitevője legfeljebb $m_1 + 1$-féle lehet: $0, 1, \ldots, m_1$ valamelyike. Ezeket a kitevőket függetlenül választhatjuk minden tagban, és így a tagok száma tényleg legfeljebb $(m_1 + 1)^n$ lehet.

2.7.3. Igaz. Ha ugyanis két változót megcserélünk, akkor egy k-adfokú P tag egy szintén k-adfokú Q tagba fog átmenni. Mivel a polinom szimmetrikus, Q is tagja lesz, és persze ugyanabban a homogén komponensben lesz, mint P. Tehát a k-adfokú homogén komponens is szimmetrikus.

2.7.4. Az $x_1x_2^3x_3$ nem lehet tag, mert akkor a szimmetria miatt tag lenne $x_1^3x_2x_3$ is, ami a főtagnál lexikografikusan nagyobb. Tehát minden kitevő legfeljebb 2 lehet (mint azt a 2.7.2. Gyakorlatban is láttuk). Emiatt hatodfokú tag csak $rx_1^2x_2^2x_3^2$ lehetne, de ez sem szerepelhet, mert ez is lexikografikusan nagyobb lenne a főtagnál. Vagyis minden tag $x_1^{m_1}x_2^{m_2}x_3^{m_3}$ alakú lesz, ahol az m_1, m_2, m_3 kitevők mindegyike legfeljebb 2 (vagyis háromféle), és az egyik legfeljebb 1. A tagok száma így maximum $3 \cdot 3 \cdot 3 - 1 = 26$ lehet (azért 1-et kell levonni, mert $x_1^2x_2^2x_3^2$ az egyetlen, ahol mindegyik kitevő legfeljebb 2, de egyik sem legfeljebb 1). Ilyen polinom létezik is, például adjuk össze 1 együtthatóval a most leírt tulajdonságú 26 tagot.

Az eljárás első lépése az, hogy le kell vonni a $\sigma_1^{2-2}\sigma_2^{2-1}\sigma_3^1 = \sigma_2\sigma_3$ tagot.

2.7.5. Az alaptétel bizonyításának egyértelműségre vonatkozó része alapján először ki kell számolni minden tagban a kitevők összegét, azaz a tagok fokát, és csak a legnagyobb fokú tagokat megtartani. Ezt már megtettük a 2.6.3. Gyakorlat megoldásában, ekkor a p_5 polinomot kapjuk. A második lépésben p_5 minden tagjában az x_2, x_3, x_4 fokait kell összeadni. Ennek legnagyobb értéke 4 lesz, és ezt csak egyetlen tagban, az $ix_1x_2x_3x_4^2$-ben érjük el. Amikor tehát x_i helyére σ_i-t írunk, akkor $i\sigma_1\sigma_2\sigma_3\sigma_4^2$ főtagja (ami a 2.7.1. Gyakorlat szerint $ix_1^5x_2^4x_3^3x_4^2$) biztosan nem fog kiesni.

2.7.6. A polinom főtagja $x_1^2x_2$, tehát első lépésben $\sigma_1^{2-1}\sigma_2^{1-0} = \sigma_1\sigma_2$-t kell levonnunk. Ehhez el kell végezni a 2.1.2. Gyakorlat alapján a $\sigma_1\sigma_2$ szorzást. Az eredmény $x_ix_jx_k$ alakú tagok összege, ahol x_i-t σ_1-ből, x_jx_k-t σ_2-ből választjuk. Így biztosan $j \neq k$. Ha i különbözik j-től is és k-tól is, akkor σ_3 egy tagját kapjuk, de hányszor? Például az $x_1x_2x_3$ tag fellép úgy is, hogy x_1-et választjuk σ_1-ből, és x_2x_3-at σ_2-ből, de felléphet úgy is, hogy σ_1-ből az x_2-t, vagy az x_3-at választjuk. Tehát $x_1x_2x_3$ (és minden ugyanilyen tag) háromszor lép fel. A másik lehetőség az, hogy i megegyezik j vagy k valamelyikével. Most tehát azt kell megszámolni, hogy mondjuk az $x_1x_2^2$ hányféleképpen kapható meg. Látjuk, hogy ez csakis $x_2(x_1x_2)$ alakban keletkezhet (hiszen a σ_2-beli tagok két indexe mindenképpen különböző). Odáig jutottunk tehát, hogy

$$\sigma_1\sigma_2 = 3\sigma_3 + f(x_1, \ldots, x_n)\,.$$

Így $f(x_1, \ldots, x_n) = \sigma_1\sigma_2 - 3\sigma_3$.

Megjegyezzük, hogy a kapott képlet $n = 2$ esetén is érvényes, ha ekkor σ_3 értékét nullának tekintjük. Ha $n = 1$, akkor a feladatban üres összeg szerepel, de a képletünk ilyenkor is helyes (ekkor σ_2 is nulla).

2.7.7. A reciprokösszeg σ_{n-1}/σ_n (ezt közös nevezőre hozással már a 2.5.9. Gyakorlatban láttuk az $n = 4$ speciális esetben). A gyökök és együtthatók összefüggése (a 2.5.5. Következmény) miatt az $x^n + x + 1$ polinom esetében $\sigma_n = (-1)^n$ és $\sigma_{n-1} = (-1)^{n-1}$, vagyis a gyökök reciprokösszege -1.

A köbösszeg meghatározására két megoldást is mutatunk. Az első megoldásban közvetlenül alkalmazzuk az alaptétel bizonyításában tanult algoritmust. Mivel a köbösszeg főtagja x^3, első lépésben a σ_1^3-t kell levonni belőle. Emeljük tehát köbre az $(x_1 + \cdots + x_n)$ összeget. Ezt a 2.1.4. Gyakorlat szerint úgy tehetjük meg, hogy az $x_1, \ldots, x_n$ közül kiválasztunk tetszőleges módon hármat, ezeket összeszorozzuk, és a kapott szorzatokat összeadjuk. Ilyenkor háromféle szorzat keletkezik. Az x_i^3 csak egyszer, az $x_i^2 x_j$ (ahol $i \neq j$) háromszor (úgy, mint $x_i x_i x_j$, $x_i x_j x_i$, $x_j x_i x_i$), végük az $x_i x_j x_k$ (ahol az i, j, k páronként különböző) hatszor (az indexeknek ugyanis hatféle lehetséges sorrendje van). De az $x_i^2 x_j$ alakú tagok összegét meghatároztuk az előző feladatban. Ennek eredményét felhasználva

$$\sigma_1^3 = s_3 + 3(\sigma_1\sigma_2 - 3\sigma_3) + 6\sigma_3\,,$$

és így $s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Itt vigyázni kell az $n = 2$ esettel, amikor a képlet csak abban az értelemben marad helyes, ha ilyenkor σ_3 értékét nullának tekintjük. Az $x^n + x + 1$ polinomból ennek alapján leolvasható, hogy a gyökök köbeinek összege $n = 2$-re 2, $n = 3$-ra és 4-re -3, $n \geq 5$-re 0.

A második megoldásban a Newton-Girard formulákat (2.7.4. Tétel) alkalmazzuk:

$$s_3 - \sigma_1 s_2 + \sigma_2 s_1 - 3\sigma_3 = 0\,.$$

Tudjuk, hogy $s_1 = \sigma_1$, továbbá akár a Newton-Girard formulákból, akár a 2.5.8. Gyakorlatból, hogy $s_2 = \sigma_1^2 - 2\sigma_2$. Ezeket behelyettesítve s_3-ra az imént már kiszámított eredmény adódik. A köbösszeget még egy harmadik módon is meghatározzuk majd a 2.7.9. Feladat megoldásában.

2.7.8. Az első keresett polinom nyilván az

$$(x - a^2)(x - b^2)(x - c^2) = x^3 - (a^2 + b^2 + c^2)x^2 + (a^2b^2 + a^2c^2 + b^2c^2)x - a^2b^2c^2$$

lesz. Az $x^3 + 3x + 1$ polinomból a gyökök és együtthatók összefüggése alapján leolvashatjuk, hogy $a + b + c = 0$, $ab + ac + bc = 3$, és $abc = -1$. Ezért nyilván $a^2b^2c^2 = (abc)^2 = 1$, és a 2.5.8. Gyakorlat alapján $a^2 + b^2 + c^2 = 0^2 - 2 \cdot 3 = -6$. Az $a^2b^2 + a^2c^2 + b^2c^2$ meghatározásához ismét az alaptétel algoritmusát használjuk fel. A főtag a^2b^2, ezért első lépésben $\sigma_2^2 = (ab+ac+bc)^2$-t kell levonni. De a négyzetösszeget ki tudjuk számítani:

$$(ab + ac + bc)^2 = a^2b^2 + a^2c^2 + b^2c^2 - 2(abac + abbc + acbc)\,,$$

és az utolsó tag nyilván $-2abc(a + b + c) = 0$. A végeredmény tehát $x^3 + 6x^2 + 9x - 1$.

A másik egyenlet esetében is okoskodhatnánk hasonlóan, de a számolás nagyon bonyolult lenne. Vegyük ehelyett észre, hogy $a+b+c=0$ miatt $a+b=-c$, $b+c=-a$, $c+a=-b$, és ezért a

$$g(x)=(x+a)(x+b)(x+c)$$

polinomot kell csak meghatároznunk. De tudjuk, hogy

$$(x-a)(x-b)(x-c)=x^3+3x+1\,.$$

Ide x helyébe $-x$-et helyettesítve, és $(-1)^3$-nel szorozva $g(x)=x^3+3x-1$ adódik.

2.7.9. A 2.6.1. Gyakorlat szerint homogén polinomok szorzata is homogén, és szorzáskor a fokok összeadódnak. Ezért $\sigma_1^{k_1}\dots\sigma_n^{k_n}$ is homogén, és foka $k_1+2k_2+\dots+nk_n$. Amikor az alaptétel bizonyításában megadott algoritmust végezzük, akkor tehát mindig egy homogén polinomot vonunk ki f-ből, melynek a foka szükségképpen annyi, mint f foka (hiszen a levont polinomot úgy választjuk, hogy a főtag mindig kiessen). Vagyis az eljárásban végig olyan tagokat vonunk le, melyekre $k_1+2k_2+\dots+nk_n=k$, és így f tényleg felírható ilyen tagok összegeként. Ha f főtagja $x_1^{m_1}\dots x_n^{m_n}$, akkor végig minden változó kitevője legfeljebb $m_1=m$ lesz. A 2.7.1. Gyakorlat szerint $\sigma_1^{k_1}\dots\sigma_n^{k_n}$-ben x_1 kitevője $k_1+k_2+\dots+k_n$, ezért minden levont tagra fenn kell álljon a $k_1+k_2+\dots+k_n\le m$ egyenlőtlenség is.

A most kapott képletek behatárolják, hogy egy adott f felírásakor az F polinomban milyen tagok szerepelhetnek egyáltalán (persze f homogén komponenseivel külön-külön kell elbánni). Illusztrációként ezzel a módszerrel is meghatározzuk az s_3 köbösszeg felírását az elemi szimmetrikus polinomokkal.

Most tehát $m=3=k$, és így $k_1+2k_2+\dots+nk_n=3$ (továbbá $k_1+\dots+k_n\le 3$, de ez kevesebbet mond ebben az esetben, mint az előző feltétel). Mivel a k_i egész számok, látjuk, hogy $k_4=\dots=k_n=0$, továbbá $k_3\le 1$ (és ha $k_3=1$, akkor $k_2=k_1=0$). Ugyanígy kapunk korlátokat k_2-re és k_1-re is, és a végén a következő lehetőségek maradnak:

$$s_3=a\sigma_3+b\sigma_2\sigma_1+c\sigma_1^3\,,$$

ahol az a, b, c együtthatók ismeretlenek. Ezeket azonban meghatározhatjuk alkalmas helyettesítésekkel is. Ha x_1 helyére 1-et, a többi határozatlan helyére nullát írunk, akkor s_3-ból és σ_1-ből 1 lesz, σ_2 és σ_3 pedig nullává válik. Ezért $c=1$. Ha $x_1=x_2=1$, és a többi változó nulla, akkor $s_3=\sigma_1=2$, $\sigma_2=1$, $\sigma_3=0$, és így a $2=2b+8$ egyenletet kapjuk, ahonnan $b=-3$. Végül x_3-at is 1-re változtatva $s_3=\sigma_1=\sigma_2=3$, $\sigma_3=1$, és a $3=a-3\cdot 3\cdot 3+27$ egyenletből $a=3$.

11.3. A polinomok számelmélete

3.1. Számelméleti alapfogalmak.

3.1.1. Az x^2+1 polinom vizsgálatához hasonlóan járunk el. Mivel $\pm\sqrt{2}$ irracionális, $\mathbb{Q}$ fölött csakis a „triviális” $x^2-2=c(x^2/c-2/c)$ felbontás létezik, ahol $c\neq 0$ racionális szám. Ezek a triviális felbontások valós c esetén $\mathbb{R}[x]$-ben is megvannak. Ugyanakkor $\mathbb{R}$ fölött $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$, és ezt a felbontást is módosíthatjuk úgy, hogy az egyik tényezőt egy valós $c\neq 0$ számmal megszorozzuk, a másikat pedig c-vel elosztjuk.

3.1.2. Ugyanúgy járunk el, mint amikor a polinomot $\mathbb{C}$ és $\mathbb{R}$ fölött vizsgáltuk. Mivel másodfokú polinomról van szó, vagy két elsőfokú szorzatára bonthatjuk, vagy pedig egy konstans, és egy másodfokú szorzatára. Ha az egyik elsőfokú tényező $ax+b$, akkor $-b/a$ gyöke a polinomnak.

A $\mathbb{Z}_2$ elemeit végigpróbálgatva azt kapjuk, hogy x^2+1 egyetlen gyöke az 1, és így $x^2+1=(x+1)(x+1)$. Ezt a felbontást módosíthatnánk még úgy, hogy az egyik tényezőt egy nem nulla konstanssal megszorozzuk, a másikat pedig ugyanezzel elosztjuk. Csakhogy $\mathbb{Z}_2$ egyetlen nem nulla eleme az 1, és így ezen a módon most nem kapunk új felbontást. Ugyanezért az x^2+1-et egy konstans és egy másodfokú polinom szorzatára is csak egyféleképpen bonthatjuk: $x^2+1=1(x^2+1)$.

A $\mathbb{Z}_3$ elemeit végigpróbálgatva azt kapjuk, hogy x^2+1-nek ebben a testben nincsen gyöke. Ezért itt az x^2+1-et csakis egy nem nulla konstans és egy másodfokú polinom szorzatára bonthatjuk: $x^2+1=1(x^2+1)=2(2x^2+2)$.

3.1.3. Mintabizonyításként csak a (3) állítást mutatjuk meg, a többi hasonlóan igazolható. Mivel $r\mid s$, az oszthatóság definíciója szerint van olyan $a\in R$, melyre $ra=s$. Ugyanígy $s\mid t$ miatt van olyan $b\in R$, hogy $sb=t$. De akkor $t=sb=(ra)b=r(ab)$, és így $r\mid t$.

3.1.4. Ha $0\mid s$, akkor van olyan $a\in R$, melyre $a\cdot 0=s$. De (a 2.2.9. Gyakorlat miatt) $a\cdot 0=0$, tehát $s=0$. Ugyanakkor $r\cdot 0=0$ miatt $r\mid 0$ tetszőleges R esetén. Ha R test, akkor $r\mid t$ mindig teljesül, kivéve ha $r=0$ de $t\neq 0$. Valóban, ha $r\neq 0$, akkor $r(t/r)=t$, ha pedig $t=0$, akkor az imént bizonyított állítás szerint t-nek minden elem osztója.

3.1.5. Ha R egységelemes, kommutatív gyűrű, akkor egy $r\in R$ (mint konstans polinom) akkor és csak akkor osztója egy $f\in R[x]$ polinomnak, ha osztója f mindegyik együtthatójának. Valóban, ha $r\mid f$, akkor van olyan $g(x)=b_0+\cdots+b_nx^n\in R[x]$, melyre

$$f(x)=rg(x)=rb_0+\cdots+rb_nx^n\,.$$

Tehát f minden együtthatója r-nek többszöröse. A megfordítás igazolásához tegyük fel, hogy $f(x)=a_0+\cdots+a_nx^n$ minden együtthatója r-rel osztható. Ekkor $a_j=rb_j$ alkalmas $b_0,\ldots,b_n\in R$ elemekre. Így

$$f(x)=r(b_0+\cdots+b_nx^n)\,,$$

vagyis $r\mid f$.

3.1.6. A három állítás azonnal adódik az oszthatóság elemi tulajdonságaiból (3.1.3. Gyakorlat): a tranzitivitás a (3)-ból, a reflexivitás a (4)-ből, a szimmetria pedig közvetlenül a definícióból.

3.1.7. Ezt már beláttuk a 2.3.2. Tételben (vagyis igazából a 2.1.5. Állításban).

3.1.8. Pozitív egész számok esetében két felbonthatatlan akkor és csak akkor asszociált, ha egyenlő. Így minden pozitív egész felírható kanonikus alakban úgy is, hogy nem szerepel egységtényező: az egyenlő felbonthatatlanokat összevonjuk. Speciálisan az 1 üres szorzatként írható (2.2.23. Gyakorlat).

Ha egy negatív egész számban egy p felbonthatatlan páratlan kitevőn szerepel, akkor p-nek a negatív asszociáltját (azaz $-|p|$-t), az összes többi szereplő felbonthatatlannak pedig a pozitív asszociáltját választva a kanonikus alakban nem lesz egységre szükség (például $-72 = (-2)^3 3^2$). A fennmaradó esetekben, vagyis ha a szám egy négyzetszám ellentettje, mindenképpen -1 lesz az egységtényező.

3.1.9. A kanonikus alak egyértelműsége precízen a következőt jelenti. Tegyük fel, hogy

$$ep_1^{\alpha_1} \dots p_m^{\alpha_m} = fq_1^{\beta_1} \dots q_n^{\beta_n},$$

ahol e, f egységek, $p_1, \dots, p_m$ páronként nem asszociált felbonthatatlanok, és $q_1, \dots, q_n$ is páronként nem asszociált felbonthatatlanok. Ekkor a $\{p_1, \dots, p_m\}$ és a $\{q_1, \dots, q_n\}$ halmazok között létezik egy kölcsönösen egyértelmű megfeleltetés úgy, hogy az egymásnak megfelelő felbonthatatlanok asszociáltak, és a kitevőik megegyeznek (speciálisan $m = n$). Vagyis ha p_i és q_j egymásnak felelnek meg, akkor $p_i \sim q_j$, és $\alpha_i = \beta_j$.

Az állítás bizonyításához az alaptétel egyértelműségi állítását használjuk fel. Mindkét oldalon felbonthatatlanok szorzata szerepel (ha az e, illetve f egységeket „beolvasztjuk" valamelyik felbonthatatlanba, például az egyik p_1 helyett ep_1-et írunk). Ezért a szereplő felbonthatatlanok között van egy kölcsönösen egyértelmű φ megfeleltetés úgy, hogy az egymásnak megfelelő felbonthatatlanok asszociáltak.

Húzzunk egy vonalat p_i és q_j között akkor, ha asszociáltak. Ekkor a φ megfeleltetés miatt minden p_i-ből és minden q_j-ből indul ki vonal. Egyikből sem indulhat ki két vonal, mert ha például p_1-ből q_1-hez és q_2-höz is vezetne vonal, akkor q_1 és q_2 asszociáltak lennének, ami nem igaz. Tehát a vonalak kölcsönösen egyértelmű megfeleltetést létesítenek $\{p_1, \dots, p_m\}$ és $\{q_1, \dots, q_n\}$ között. Be kell még látni, hogy ha $p_i \sim q_j$, akkor $\alpha_i = \beta_j$.

Ha r tetszőleges felbonthatatlan, amelynek α darab asszociáltja van a baloldalon, akkor pontosan az ezeknek φ-nél megfelelő jobboldali felbonthatatlanok lesznek r asszociáltjai a jobboldalon, és így a jobboldalon is α darab asszociáltja van r-nek. Ha tehát r asszociáltja a baloldalon p_i, a jobboldalon meg q_j, akkor $p_1 \sim q_i$, és $\alpha_i = \beta_j = \alpha$.

3.1.10. Tegyük fel, hogy az r és s elemeknek u és v is kitüntetett közös osztója. Ekkor u közös osztó, és ezért v kitüntetettsége miatt $u \mid v$. Az u és v szerepét megcserélve $v \mid u$, és így $u \sim v$.

3.1.11. Ha adott egy p felbonthatatlan, akkor bármely $r \in R$ esetében megtehetjük, hogy az r kanonikus alakjában p asszociáltjai közül éppen p-t szerepeltetjük (vagyis ha r felbontásában eredetileg p-nek egy pe asszociáltja szerepel, akkor az e egységtényezőt kivisszük a kanonikus alak elejére, és beleolvasztjuk az ottani egységbe). Az sem akadály, ha p nem is osztója r-nek, ebben az esetben p kitevője r kanonikus alakjában nulla lesz. Például ha $p = -2$, akkor $24 = (-1)(-2)^3 3^1$ és $15 = 1 \cdot (-2)^0 3^1 5^1$. Így tetszőleges két elem, r és s kanonikus alakja felírható

$$r = e p_1^{\alpha_1} \dots p_m^{\alpha_m} \quad \text{és} \quad s = f p_1^{\beta_1} \dots p_m^{\beta_m}$$

alakban, amivel az (1)-et beláttuk.

Ezekre az elemekre $r \mid s$ akkor és csak akkor, ha $\alpha_i \leq \beta_i$ minden $1 \leq i \leq m$ esetén. Valóban, ha ez a feltétel teljesül, akkor

$$s = r(f/e) p_1^{\beta_1 - \alpha_1} \dots p_m^{\beta_m - \alpha_m},$$

és itt f/e egy értelmes eleme R-nek, hiszen e egység, és így lehet vele R-ben osztani. Megfordítva, ha $r \mid s$, akkor van olyan $t \in R$, melyre $rt = s$. Így t minden felbonthatatlan osztója osztója s-nek, és így t kanonikus alakja is felírható $t = g p_1^{\gamma_1} \dots p_m^{\gamma_m}$ alakban, ahol $g \in R$ egység. A szorzást elvégezve a kanonikus alak egyértelműsége miatt $\alpha_i + \gamma_i = \beta_i$ adódik, vagyis $\alpha_i \leq \beta_i$ tényleg teljesül. Így (2) is igaz.

Most már meg tudjuk mutatni, hogy ha $\delta_i = \min(\alpha_i, \beta_i)$, akkor a fenti r és s elemeknek az $u = p_1^{\delta_1} \dots p_m^{\delta_m}$ kitüntetett közös osztója lesz. A (2) állítás szerint u közös osztó, mert a kanonikus alakjában szereplő δ_i kitevőkre $\delta_i \leq \alpha_i$ és $\delta_i \leq \beta_i$ is teljesül. Ha viszont v is közös osztója r-nek és s-nek, akkor v-nek is minden felbonthatatlan osztója valamelyik p_i asszociáltja, és így v kanonikus alakja is felírható $v = g p_1^{\gamma_1} \dots p_m^{\gamma_m}$ alakban, ahol $g \in R$ egység. Így (2) miatt $\gamma_i \leq \alpha_i$ és $\gamma_i \leq \beta_i$ minden i-re, de akkor γ_i legfeljebb akkora lehet, mint α_i és β_i közül a nem nagyobb, vagyis δ_i. Tehát (2) miatt $v \mid u$. Ezzel a kitüntetett közös osztó létezését, azaz a (3) állítást beláttuk.

Azt mondjuk, hogy az $u \in R$ elem az r és s elemek *kitüntetett közös többszöröse,* ha $r \mid u$ és $s \mid u$ (azaz u közös többszörös), és ha v tetszőleges közös többszöröse r-nek és s-nek, akkor $u \mid v$. Az eddig bizonyítottakhoz teljesen hasonlóan igazolható, hogy a fenti r és s elemeknek

$$p_1^{\max(\alpha_1, \beta_1)} \dots p_m^{\max(\alpha_m, \beta_m)}$$

kitüntetett közös többszöröse lesz. Az, hogy a kitüntetett közös többszörös asszociáltság erejéig egyértelmű, ugyanúgy igazolható, mint ahogy a kitüntetett közös osztó esetében történt a 3.1.10. Gyakorlatban.

Végül ha kettőnél több, de véges sok elem adott, akkor ezeknek is van közös kanonikus alakja. Kitüntetett közös osztót úgy kapunk, hogy minden p felbonthatatlan esetében az előforduló kitevők minimumát vesszük. Ha a maximumot vesszük, akkor az eredmény kitüntetett közös többszörös lesz.

3.1.12. Legyen R szokásos gyűrű, és $p \in R$ prím. Meg kell mutatni, hogy p felbonthatatlan. Mivel p prím, p nem nulla, és nem egység. Tegyük fel, hogy $p = rs$. Ekkor r és s is osztója p-nek. Másrészt $p \mid rs$, és így p prímtulajdonsága miatt $p \mid r$ vagy $p \mid s$. Az első esetben tehát r és p asszociáltak, a másodikban pedig s és p asszociáltak. A $p = rs$ felbontás tehát csak triviális lehet, és így p tényleg felbonthatatlan.

Most legyen R alaptételes gyűrű, és p egy felbonthatatlan eleme R-nek. Ekkor p nem nulla és nem egység, meg kell mutatni, hogy prímtulajdonságú. Tegyük fel, hogy $p \mid rs$, azaz $rs = pt$ alkalmas $t \in R$ esetén. Az r, s és t elemeket írjuk fel felbonthatatlanok szorzataként. Ha $r = p_1 \dots p_m$ és $s = q_1 \dots q_n$, akkor

$$pt = rs = p_1 \dots p_m q_1 \dots q_n \,.$$

Az R gyűrű alaptételes, így az rs elemnek a felbontása egyértelmű. Mivel p szerepel a baloldalon, ezért a jobboldalon álló tényezők valamelyike p-nek asszociáltja. Ha ez valamelyik p_i, akkor $p \mid r$, ha meg valamelyik q_j, akkor $p \mid s$. Tehát p tényleg prím. Az olvasóra bízzuk annak az esetnek a végiggondolását, amikor r vagy s valamelyike nulla (vagy egység).

3.1.13. Az oszthatóság akkor teljesül, ha van olyan $f(x) = a_0 + \dots + a_n x^n$ polinom, melyre

$$3x^2 = 2x(a_0 + \dots + a_n x^n) = 2a_0 x + 2a_1 x^2 + \dots + 2a_n x^{n+1} \,.$$

Két polinom akkor egyenlő, ha a megfelelő együtthatóik megegyeznek. Ezért $2a_1 = 3$, és $2a_i = 0$ ha $i \neq 1$. A $2a_1 = 3$ egyenletnek a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ testekben van megoldása ($a_1 = 3/2$), $\mathbb{Z}$-ben azonban nincs. Tehát az oszthatóság nem igaz $\mathbb{Z}[x]$-ben, a másik három esetben azonban igen: $3x^2 = (2x)\big((3/2)x\big)$.

Megjegyezzük, hogy polinomok között az oszthatóságot általában nem ezzel a módszerrel érdemes eldönteni, hanem a következő, 3.2. Szakaszban tárgyalt maradékos osztási eljárás segítségével.

3.1.14. Ha $r \mid s$, akkor (r, s) (asszociáltság erejéig) r lesz, hiszen r közös osztó, és ha t is közös osztó, akkor $t \mid r$ miatt r kitüntetett is. Speciálisan r és 0 kitüntetett közös osztója r (és r asszociáltjai), hiszen $r \mid 0$.

3.1.15. Triviális felbontást eleve csak nem nulla elem esetében definiáltunk. A nulla ugyanis túl „furcsán” viselkedik: a $0 = 0 \cdot 0$ felbontásban például mindkét tényező a 0-nak asszociáltja, de egyik tényező sem egység. Nullosztómentes gyűrűben az igaz, hogy a nulla minden felbontásában az egyik tényező a nullának asszociáltja lesz (tudniillik önmaga). Egy egység minden felbontása triviális, hiszen minden tényező egység lesz.

Egy R gyűrűben a $0 \mid rs$-ből akkor és csak akkor következik, hogy $0 \mid r$ vagy $0 \mid s$, ha R nullosztómentes (hiszen $0 \mid t$ akkor és csak akkor, ha $t = 0$). Minden egységre teljesül, hogy ha osztója egy szorzatnak, akkor osztója valamelyik (sőt mindegyik) tényezőnek.

3.1.16. Tegyük fel, hogy R alaptételes. Írjuk fel az r, s, t számokat közös kanonikus alakban:

$$r = ep_1^{\alpha_1} \dots p_m^{\alpha_m}, \quad s = fp_1^{\beta_1} \dots p_m^{\beta_m}, \quad t = gp_1^{\gamma_1} \dots p_m^{\gamma_m}.$$

A 3.1.11. Gyakorlatban a kitüntetett közös osztóra kapott képlet szerint ekkor a p_i kitevője az $(r, s)t$-ben $\min(\alpha_i, \beta_i) + \gamma_i$, az (rt, st)-ben pedig $\min(\alpha_i + \gamma_i, \beta_i + \gamma_i)$ lesz. Elég tehát belátni a

$$\min(\alpha, \beta) + \gamma = \min(\alpha + \gamma, \beta + \gamma)$$

azonosságot. Ez könnyen ellenőrizhető esetszétválasztással: ha $\alpha \leq \beta$, akkor mindkét oldal $\alpha + \gamma$, egyébként pedig mindkét oldal $\beta + \gamma$.

Az minden szokásos gyűrűben igaz, hogy $(r, s)t$ osztója (rt, st)-nek. Valóban, $(r, s) \mid r$ miatt $(r, s)t \mid rt$, ugyanígy $(r, s)t \mid st$, és így (rt, st) kitüntetettsége miatt $(r, s)t \mid (rt, st)$. Ha viszont tudjuk, hogy $(r, s) = rx + sy$, akkor innen $(r, s)t = rtx + sty$. Ezt pedig osztja (rt, st), hiszen osztja rt-t és st-t is. Így tehát $(r, s)t$ és (rt, st) egymás osztói, vagyis asszociáltak.

3.1.17.

Akinek még nehézséget okoz általános gyűrűben gondolkozni, az az alábbi megoldásban nyugodtan gondoljon pozitív egészekre, és ennek megfelelően helyettesítse a $\sim$ jelet $=$ jellel (tehát asszociáltság helyett mondjon egyenlőséget), egység helyett pedig 1-et.

Tegyük fel, hogy $r \mid st$ és $(r, s) \sim 1$. A kitüntetett közös osztó kiemelési tulajdonsága miatt (rt, st) és $(r, s)t$ asszociáltak. Mivel r és s relatív prímek, $(r, s)t \sim t$. Másfelől r közös osztója rt-nek és st-nek, vagyis $r \mid (rt, st) \sim (r, s)t \sim t$. Tehát tényleg $r \mid t$, és így (1)-et beláttuk.

Most legyen p irreducibilis elem. Ekkor p nem nulla, nem egység, és mindegyik osztója vagy egység, vagy p-nek asszociáltja. Tegyük fel, hogy $p \mid rs$, de $p \nmid r$. Ekkor (p, r) osztója p-nek, de nem lehet p-nek asszociáltja (mert akkor $p \sim (p, r) \mid r$ miatt $p \mid r$ teljesülne). Mivel p irreducibilis, $(p, r) \mid p$ csak egység lehet. Az (1) tulajdonság szerint tehát $p \mid t$.

3.1.18. Tegyük fel, hogy $f = p_1 \dots p_k = q_1 \dots q_\ell$ az $f \in R$ elem két felbontása irreducibilisek szorzatára. A feltevés szerint p_1 prím, és mivel osztója a $q_1 \dots q_\ell$ szorzatnak, osztója valamelyik q_j-nek. De q_j irreducibilis, p_1 pedig nem egység, és így $p_1 \sim q_j$. Vagyis $q_j = p_1 e_1$ valamilyen e_1 egységre. Rendeljük hozzá p_1-hez q_j-t, és mindkét oldalt egyszerűsítsük p_1-gyel. Ezután p_2-vel folytatjuk az eljárást. Amikor az összes p_i elfogyott, akkor a baloldalon 1 marad, a jobboldalon pedig az e_i egységeknek és még esetleg néhány q_j-nek a szorzata. De minden ilyen megmaradó q_j osztója lenne 1-nek, ami nem lehet (hiszen q_j irreducibilis, tehát nem egység). Ezért a p_i-k és a q_j-k egyszerre fogynak el, és így a közöttük most felépített leképezés kölcsönösen egyértelmű.

3.1.19. Ismét a 3.1.11. Gyakorlatban a kitüntetett közös osztóra és a kitüntetett közös többszörösre kapott képlet segítségével számolunk, ekkor mindegyik kitevőben a

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$$

azonosságot kell igazolni. Ez pedig teljesül, hiszen ha két szám közül a kisebbet hozzáadjuk a nagyobbhoz, akkor a két szám összegét kapjuk.

3.1.20. Tudjuk a 2.2.15. (2) Gyakorlat megoldásából, hogy a Gauss-egészek között négy egység van: a ± 1 és a $\pm i$. Határozzuk meg a 2 osztóit ugyanezzel a gondolatmenettel. Ha $(a + bi)(c + di) = 2$, akkor ezt az egyenletet a konjugáltjával megszorozva

$$(a^2 + b^2)(c^2 + d^2) = 4$$

adódik. Ha itt $a^2 + b^2 = 1$, akkor az idézett megoldásban láttuk, hogy $a + bi$ egység. Ugyanígy ha $c^2 + d^2 = 1$, akkor $c + di$ egység, és akkor $a + bi$ értéke $2, -2, 2i$, vagy $-2i$ lesz. Ezek tehát a 2 triviális felbontásai. Az egyetlen további lehetőség, ha $a^2 + b^2 = 2$. Ekkor a és b is csak ± 1 lehet, és $a + bi$-re $1 + i,\ 1 - i,\ -1 + i,\ -1 - i$ adódik (vagyis az $1 + i$ négy asszociáltja). Így végülis 2 osztói $1, 1 + i, 2$, és ezek asszociáltjai.

Most meg kell néznünk, hogy ezek közül melyek osztják $1 + 3i$-t. Az 1 nyilván osztja, a 2 nem, mert ha $2(u + vi) = 1 + 3i$, akkor innen $2u = 1$ (és $2v = 3$), ami u és v egészekre lehetetlen. Végül az $(1 + 3i)/(1 + i)$ osztást elvégezve $2 + i$ adódik, ami Gauss-egész. Tehát $1 + i \mid 1 + 3i$, és így a 2 és az $1 + 3i$ kitüntetett közös osztói $1 + i$ asszociáltjai.

A fenti meggondolást praktikusan csak kis számokra lehet végrehajtani. Azonban a Gauss-egészek között is el lehet végezni a maradékos osztást, és az euklideszi algoritmust is, amivel általában is meg tudjuk határozni két Gauss-egész kitüntetett közös osztóját. Érvényes az alaptétel is, és ez az egyik kiindulópontja érdekes, egész számokra vonatkozó tételek bizonyításának. Az érdeklődő olvasó minderről a [**4**] könyv 7.4. Szakaszában olvashat.

3.1.21. Legyen R kommutatív, nullosztómentes gyűrű. Belátjuk, hogy ha egy $r \neq 0$ elem osztója önmagának, akkor R egységelemes. Valóban, ekkor van olyan $x \in R$, hogy $rx = r$. A 2.4.16. Gyakorlat megoldásához hasonlóan innen $rxs = rs$, majd r-rel egyszerűsítve $xs = s$ teljesül minden $s \in R$ esetén, azaz x egységeleme R-nek.

Ha tehát $e \in R$ minden elemnek osztója, akkor $e \mid e$ miatt R egységelemes, kivéve ha $e = 0$, amikor a 2.2.9. Feladat szerint R a nullgyűrű. Ha $p \in R$ prím, akkor $p \mid p^2$-ből a prímtulajdonság miatt $p \mid p$ következik, és így most is azt kapjuk, hogy R egységelemes. Ha r és s asszociáltak, akkor $r \mid s \mid r$ miatt $r \mid r$, és így ha R nem egységelemes, akkor $r = 0$. Így $r \mid s$ miatt $s = 0$, vagyis az egyetlen asszociált elempár a $(0, 0)$.

A páros számok nyilván részgyűrűt alkotnak $\mathbb{Z}$-ben, amely nem egységelemes, hiszen a $2x = 2$ egyenletnek $\mathbb{Z}$-ben is csak az 1 szám megoldása. A felbonthatatlanok a néggyel ($\mathbb{Z}$-ben) nem osztható számok (vagyis a $4k + 2$ alakú számok, ahol $k \in \mathbb{Z}$). Ezek valóban felbonthatatlanok, hiszen két páros szám szorzata biztosan osztható néggyel. Megfordítva, ha egy nem nulla szám néggyel osztható $\mathbb{Z}$-ben, vagyis $4k$ alakú, akkor $2(2k)$ a páros számok körében készített felbontása, amely nemtriviális (hiszen nem nulla számnak ebben a gyűrűben nincs is asszociáltja).

Ezek szerint minden páros szám felbontható a páros számok gyűrűjében felbonthatatlanok szorzatára: ha a $\mathbb{Z}$-beli kanonikus alakjában 2^n szerepel, akkor $n-1$ darab kettest kiemelve a megmaradó tényező is felbonthatatlan lesz. A felbontás nem egyértelmű, hiszen például $36 = 2\cdot 18 = 6\cdot 6$ két lényegesen különböző felbontás felbonthatatlanok szorzatára (mert a 2 nem asszociáltja a 6-nak).

Ha a 3.1.2. Definíció utáni megjegyzésben leírt asszociáltság-fogalmat használjuk, akkor a páros számok gyűrűjében két elem akkor és csak akkor lesz asszociált, ha egyenlők.

3.1.22. A 2 konstans polinom osztói $\mathbb{Z}[x]$-ben csak ± 1 és ± 2 (hiszen ha $2 = pq$, akkor p és q is csak nulladfokú lehet). Ezek közül x-et ± 1 osztja, ± 2 nem. Tehát 2 és x közös osztói csak ± 1, és így ezek kitüntetettek is. Ha $2p(x)+xq(x) = 1$ lenne alkalmas $p, q \in \mathbb{Z}[x]$-re, akkor $x = 0$-t helyettesítve $2p(0) = 1$, ami lehetetlen, mert $p(0)$ egész szám.

3.1.23. Ha a 3 prím lenne R-ben, akkor a $3\cdot 3 = 9 = (2+i\sqrt{5})(2-i\sqrt{5})$ összefüggés miatt osztaná $2+i\sqrt{5}$ és $2-i\sqrt{5}$ valamelyikét. De ha például $3(a+bi\sqrt{5}) = 2+i\sqrt{5}$ lenne, akkor a valós részeket véve $3a = 2$, ami egész a-ra nem teljesül. Tehát a 3 nem prím.

A 3 osztóinak megkereséséhez a 3.1.20. Gyakorlat mintájára járunk el. Tegyük fel, hogy

$$(a+bi\sqrt{5})(c+di\sqrt{5}) = 3\,.$$

Ezt az egyenletet a konjugáltjával megszorozva

$$(a^2+5b^2)(c^2+5d^2) = 9$$

adódik (és e két tényező pozitív egész). Tehát csak a $9 = 1\cdot 9 = 3\cdot 3 = 9\cdot 1$ felbontás jön szóba. De $a^2+5b^2 \geq 5$, ha $b \neq 0$. Ezért a^2+5b^2 soha nem lesz 3 (mert az nem négyzetszám), és 1 is csak úgy lehet, ha $a+bi\sqrt{5} = \pm 1$. Mivel a ± 1 egységek, a 3 mindegyik felbontása triviális.

Tehát 3 osztói csak ± 1 és ± 3 lesznek. Láttuk, hogy ± 3 nem osztója $2+i\sqrt{5}$-nek. Így csak a ± 1 közös osztója 3-nak és $2+i\sqrt{5}$-nek, ezek persze kitüntetettek is. Tegyük fel, hogy R-ben teljesül a kitüntetett közös osztó kiemelési tulajdonsága. Ekkor

$$\big((2-i\sqrt{5})3,\,(2-i\sqrt{5})(2+i\sqrt{5})\big) \sim (2-i\sqrt{5})\big(3,\,2+i\sqrt{5}\big) = \pm(2-i\sqrt{5})\,.$$

De ez nem igaz: $\big((2-i\sqrt{5})3,\,(2-i\sqrt{5})(2+i\sqrt{5})\big) = \big((2-i\sqrt{5})3,\,9\big)$ osztható 3-mal (hiszen a 3 közös osztója $(2-i\sqrt{5})3$-nak és 9-nek), $2-i\sqrt{5}$ pedig nem osztható 3-mal.

3.1.24. Ez a halmaz nyilván zárt az összeadásra és az ellentettképzésre, és tartalmazza a konstans polinomokat is. Ha két ilyen polinomot összeszorzunk, akkor a szorzatban a konstans tagon kívül csupa legalább $3+3 = 6$-odfokú tag lesz, és így a szorzat is benne van a halmazban. A 2.2.10. Feladat miatt tehát R tényleg részgyűrű. De $1 \in R$, és mivel $\mathbb{R}[x, y]$ szokásos gyűrű, R is nullosztómentes és kommutatív.

Belátjuk, hogy az x^5y^2 és az x^2y^5 polinomoknak nincs kitüntetett közös osztója. Tegyük fel ugyanis, hogy $p \in R$ kitüntetett közös osztó. Ekkor p osztója x^5y^2-nek $\mathbb{R}[x, y]$-ban is, és ezért könnyen láthatóan cx^ny^m alakú, ahol $c \in \mathbb{R}$, $n \leq 5$ és $m \leq 2$. Mivel $p \mid x^2y^5$, ezért $n \leq 2$ is teljesül. Másrészt viszont x^2y közös osztója x^5y^2-nek és x^2y^5-nak az R

gyűrűben (hiszen $x^5y^2/x^2y = x^3y$ és $x^2y^5/x^2y = y^4$ is elemei R-nek), ezért $x^2y \mid p$. Ez azt jelenti, hogy $n \geq 2$. Ugyanígy $xy^2 \mid p$, és így $m \geq 2$. De akkor $p = cx^2y^2$, ami lehetetlen, mert $cx^2y^2 \notin R$.

3.1.25. Azt, hogy R szokásos gyűrű, ugyanúgy láthatjuk be, mint ahogy $\mathbb{R}[x]$-ről megmutattuk, hogy szokásos gyűrű: itt is igaz lesz, hogy a főtagok szorzata a szorzat főtagja. Megmutatjuk, hogy x-nek minden osztója cx^r alakú, ahol $c \in \mathbb{R}$, és $0 \leq r \leq 1$ valós szám.

Valóban, ha $pq = x$, akkor a főtagokat összeszorozva x-et kell, hogy kapjunk, és így ha p főtagja cx^r, q főtagja pedig dx^s, akkor $cd = 1$ és $r + s = 1$. Legyen p, illetve q „altagja", azaz legalacsonyabb „fokú" tagja $c'x^{r'}$, illetve $d'x^{s'}$. A szorzatpolinom képletéből láthatjuk, ugyanúgy, mint a főtagok esetében, hogy a pq szorzat „altagja" $c'd'x^{r'+s'}$ lesz, és ez most szintén x. Emiatt $r' + s' = 1$, de $r' \leq r$ és $s' \leq s$ miatt ez csak úgy lehetséges, ha $r' = r$ és $s' = s$. Vagyis a p és a q polinom is csak egyetlen tagból állhat.

Így viszont x-et nemhogy nem tudjuk felbonthatatlanok szorzatára bontani, de még felbonthatatlan osztója sincs! Ugyanis cx^r felírható $cx^{r/2}$ és $x^{r/2}$ szorzataként, és (ha $r > 0$, akkor) ez nemtriviális felbontás, hiszen R egységei a nem nulla konstans polinomok. (Ha $r = 0$, akkor viszont cx^r egység, tehát ismét nem felbonthatatlan.)

3.2. A maradékos osztás.

3.2.1. Ugyanígy bizonyítunk, mint az egész számok számelméletében. A 90. oldalon található jelöléseket használjuk. Elsőnek azt mutatjuk meg, hogy r_n közös osztója f-nek és g-nek. Az utolsó sorból látszik, hogy $r_n \mid r_{n-1}$. Az utolsó előtti sor szerint $r_n \mid r_{n-2}$. Ugyanígy haladunk tovább felfelé: ha már tudjuk, hogy r_n osztója r_{j+1}-nek és r_j-nek is, akkor azt a sort használva, amelynek a baloldalán r_{j-1} áll, azt kapjuk, hogy $r_n \mid r_{j-1}$. A második sorhoz érve $r_n \mid g$, végül az első sorból $r_n \mid f$ adódik.

Az r_n kitüntetettségének igazolásához tegyük fel, hogy $r \mid f$ és $r \mid g$ is teljesül. Az első sorból ekkor $r \mid r_1$. A második sorból ezt felhasználva $r \mid r_2$. Lefelé haladva sorban látjuk, hogy $r \mid r_j$ minden j-re, végül az utolsó előtti sor adja a kívánt $r \mid r_n$ összefüggést.

Végül az r_n-et előállítjuk $fp + gq$ alakban. Ismét alulról fölfelé haladunk. Az utolsó előtti sor szerint $r_n = r_{n-2} - r_{n-1}q_n$. Ide behelyettesítjük az r_{n-1}-nek az alulról a harmadik sorból kapott $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$ előállítását:

$$r_n = r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = r_{n-3}(-q_n) + r_{n-2}(1 + q_{n-1}q_n)\,.$$

Vagyis az r_n-et most már r_{n-3} és r_{n-2} segítségével állítottuk elő. Ha most r_{n-2}-t fejezzük ki az alulról számított negyedik sorból, és ide behelyettesítünk, akkor r_n-nek az r_{n-4} és r_{n-3} segítségével kapott előállítását kapjuk. Az eljárást folytatva végül r_n-et f és g segítségével felírva kapjuk meg.

Azt tanácsoljuk az olvasónak, hogy ezt a *visszahelyettesítési eljárást* ne általában próbálja megérteni, hanem először két konkrét pozitív egész számra végezze el. Ezután érdemes ugyanezt polinomokkal is kipróbálni, erre szolgál a 3.2.9. Gyakorlat. A most leírt eljárás hangsúlyozottan a p és q megkeresésére szolgál, ha csak azt akarjuk megmutatni, hogy létezik ilyen p és q, akkor inkább a 3.2.3. Tétel bizonyítását érdemes követni.

3.2.2. Először praktikusan vizsgáljuk a kérdést. Ha f és g valamelyike nulla, akkor persze a kitüntetett közös osztójuk a másik lesz. Általánosabban, ha az egyik osztója a másiknak, például $g \mid f$, akkor a kitüntetett közös osztó g lesz. Ez persze nem látszik ránézésre, csak ha az osztást elvégezzük. Természetesen a nagyobb fokút érdemes osztani a kisebb fokúval, vagyis ha véletlenül $\mathrm{gr}(f) < \mathrm{gr}(g)$, akkor meg kell cserélni a két polinomot. Ha már az első osztás maradéka, $r_1 = 0$, akkor a kitüntetett közös osztó g lesz.

A fenti diszkusszió nagy részét elkerülhetjük, ha a $g = r_0$ (sőt $f = r_{-1}$) jelölést bevezetjük. Ez azonban, bár formálisan megoldaná a problémákat, a szőnyeg alá söpörné az előző bekezdésben megvizsgált kérdéseket.

3.2.3. Az euklideszi algoritmus elvégzése során minden számítás ugyanaz lesz, akár $\mathbb{Q}$, akár $\mathbb{C}$ fölött gondolkozunk (hiszen a számításokban csak a négy alapműveletet használjuk), ezért a végeredmény, azaz a kitüntetett közös osztó is ugyanaz. Természetesen a kitüntetett közös osztó csak konstansszoros erejéig egyértelmű, vagyis a kapott racionális együtthatós polinom nem nulla racionális konstansszorosai lesznek kitüntetett közös osztók $\mathbb{Q}[x]$-ben, és a nem nulla komplex konstansszorosai lesznek kitüntetett közös osztók $\mathbb{C}[x]$-ben. Ezért *minden* $\mathbb{Q}$ fölötti kitüntetett közös osztó egyben $\mathbb{C}$ fölött is az.

Az általánosítás a következő. Legyen T test, és S részteste T-nek. Ha h kitüntetett közös osztója az $f, g \in S[x]$ polinomoknak $S[x]$-ben, akkor h az f és g kitüntetett közös osztója $T[x]$-ben is. A bizonyítás ugyanaz, mint az előző bekezdésben.

3.2.4. Elképzelhető, hogy I csak a nullapolinomból áll, és ekkor nincsen benne legalacsonyabb fokú polinom (mert az egyetlen elemének nincs foka). De ebben az esetben a $h_0 = 0$ választás megfelelő lesz, hiszen ennek többszörösei kiadják I összes elemét. Természetesen $f, g \in I$ miatt ez az eset csak akkor fordulhat elő, ha $f = g = 0$, amikor a Tétel állítása közvetlenül is nyilvánvaló.

3.2.5. Nem irreducibilis, a $2x = 2 \cdot x$ nemtriviális felbontás. Ugyanis $\mathbb{Z}[x]$ egységei a 3.1.7. Gyakorlat szerint csak ± 1, és így sem 2, sem x nem lesz egység.

3.2.6. A 3.2.1. Gyakorlat (vagy a 3.2.3. Tétel) szerint egy T test feletti $T[x]$ polinomgyűrűben f és g kitüntetett közös osztója felírható $fp + gq$ alakban alkalmas p, q polinomokra. A 3.1.16. Gyakorlat miatt tehát érvényes a kitüntetett közös osztó kiemelési tulajdonsága, és így a 3.1.17. Gyakorlat mutatja, hogy $T[x]$ minden irreducibilis eleme prím. Végül a 3.1.18. Feladat adja az alaptétel egyértelműségi állítását.

3.2.7. Tegyük fel, hogy van olyan nem konstans polinom $T[x]$-ben, amely nem bontható fel irreducibilisek szorzatára. Válasszunk ezek közül egy minimális fokszámú f polinomot. A minimalitás tehát azt jelenti, hogy az f-nél kisebb fokú polinomok már mind felbomlanak irreducibilisek szorzatára. Az f nem lehet irreducibilis, hiszen akkor önmaga, mint egytényezős szorzat az f-nek irreducibilisekre való felbontása lenne. Ezért f felbomlik az f-nél alacsonyabb fokú g és h polinomok szorzatára. Az f fokának a minimalitása miatt g és h már felbomlik irreducibilisek szorzatára: $g = p_1 \dots p_n$ és $h = q_1 \dots q_m$. De akkor $f = p_1 \dots p_n q_1 \dots q_m$ az f-nek irreducibilisek szorzatára való felbontása. Ez

ellentmondás, ezért ilyen f polinom nincs, és így minden nem konstans $T[x]$-beli polinom irreducibilis polinomok szorzatára bomlik.

3.2.8. A hányados $x/2 - 1/2$, a maradék $(5/2)x - (7/2)$.

3.2.9. Az eredmények a következők.

(1) A kitüntetett közös osztó $x^2 + x + 1$ (illetve ennek bármelyik konstansszorosa), és

$$x^2 + x + 1 = \big(-(1/9)x + (2/9)\big)f(x) + (1/6)g(x)\,.$$

(2) Itt három osztást kell elvégezni. A kitüntetett közös osztó

$$x - 1 = (-x)(x^5 - 1) + (1 + x^3)(x^3 - 1)\,.$$

3.2.10. Nem végezhető el. Az osztónak, vagyis a konstans 2 polinomnak a foka 0, ennél r foka kisebb nem lehet. Ezért r a nullapolinom, vagyis $x = 2q(x)$. De ez lehetetlen: az x polinom nem osztható 2-vel $\mathbb{Z}[x]$-ben, mert egy polinom itt akkor és csak akkor osztható 2-vel, ha mindegyik együtthatója páros (3.1.5. Gyakorlat).

3.2.11. Igaz, a maradékos osztás $\mathbb{Q}[x]$-beli egyértelműsége miatt. Ha ugyanis $g = fh$, ahol $h \in \mathbb{Z}[x]$, akkor $g = fh + 0$ egy maradékos osztás $\mathbb{Q}[x]$-ben, tehát az eljárásnak ezt kell kihoznia.

3.2.12. A lényeg most is az, hogy az osztási eljárás során végig minden együttható S-ben lesz, hiszen most g főegyütthatójával lehet S-ben osztani. A 3.2.2. Állítás bizonyításához hasonlóan tehát a következőképpen haladhatunk. Mivel g főegyütthatója invertálható S-ben, ezért itt lehet vele maradékosan osztani: $f = gq_1 + r_1$, ahol $q_1, r_1 \in S[x]$, és $r_1 = 0$, vagy r_1 foka kisebb g fokánál. Ugyanakkor $f = gq + 0$ alkalmas $q \in T[x]$ polinomra, hiszen g osztója f-nek $T[x]$-ben. A maradékos osztás egyértelműségét $T[x]$-ben alkalmazva ($q = q_1$ és) $0 = r_1$ adódik, azaz g osztója f-nek $S[x]$-ben is.

3.2.13. Az f polinomot $x - b$-vel osztva $f(x) = (x - b)q(x) + r$ adódik, ahol r konstans. Az x helyére b-t helyettesítve $r = f(b)$. Speciálisan $f(b) = 0$ akkor és csak akkor, ha f osztható $x - b$-vel.

3.2.14. Nulla lesz a maradék. Ha csak a maradékra vagyunk kíváncsiak, és az osztó nagyon kis fokú polinom, melynek a gyökeit ismerjük, akkor ezeknek a gyököknek a behelyettesítése segíthet a maradék megkeresésében. A legegyszerűbb példát erre az előző gyakorlatban láttuk: f-et $x - b$-vel osztva a maradék $f(b)$ lesz.

Most másodfokú polinommal osztunk, ezért a maradék $ax + b$ alakú polinom:

$$x^4 + x^2 + 1 = (x^2 + x + 1)q(x) + (ax + b)$$

(ahol a és b valós, sőt racionális számok, hiszen az osztandó és az osztó is racionális együtthatós). Az $x^2+x+1 = (x^3-1)/(x-1)$ polinom gyökei a primitív harmadik egységgyökök: $\varepsilon_1 = \cos 120^\circ + i \sin 120^\circ$, és $\varepsilon_2 = \cos 240^\circ + i \sin 240^\circ$. Mivel $\varepsilon_i^4 = \varepsilon_i$, ezek gyökei az $x^4 + x^2 + 1$ polinomnak is. Ezért behelyettesítve $a\varepsilon_i + b = 0$ adódik. A két egyenletet kivonva $a(\varepsilon_1 - \varepsilon_2) = 0$, és mivel $\varepsilon_1 - \varepsilon_2 \neq 0$, ezért $a = 0$, és $a\varepsilon_i + b = 0$-ból $b = 0$.

Ezt az észrevételt többféleképpen is általánosíthatjuk. Például az $x^4 + x^2 + 1$ helyett vehetjük az $f(x) = x^{2n} + x^n + 1$ polinomot. Ha n nem osztható 3-mal, akkor f-nek is gyöke lesz ε_1 és ε_2, és így a leírt gondolatmenet alapján f is osztható $x^2 + x + 1$-gyel.

3.2.15. Itt már nem praktikus a maradékos osztás elvégzése, az előző gyakorlat megoldásában látott technikát alkalmazzuk. Legyen

$$x^{64} + x^{54} + x^{14} + 1 = (x^2 - 1)q(x) + (ax + b)\,.$$

Az x helyébe 1-et és -1-et helyettesítve $a + b = 4$ és $-a + b = 4$ adódik, ahonnan $a = 0$, $b = 4$, tehát a maradék 4.

Az $x^2 + 1$-gyel való osztáskor i-t és $-i$-t érdemes helyettesíteni. Az i-t behelyettesítve $ai + b = 0$ adódik. Itt a, b valós (sőt mellesleg egész, hiszen az osztó, $x^2 + 1$ főegyütthatója invertálható $\mathbb{Z}$-ben). Ezért $ai + b = 0$-ból azt kapjuk, hogy $a = b = 0$, vagyis az osztásnál a maradék nulla.

3.2.16. A b gyök h-beli multiplicitása az f-beli és a g-beli multiplicitások minimuma lesz. Ha ugyanis b multiplicitása f-ben k és g-ben ℓ, ahol mondjuk $k \leq \ell$, akkor $(x - b)^k$ közös osztója f-nek és g-nek, és így osztója h-nak is. De h-ban nem lehet b multiplicitása k-nál nagyobb, hiszen $h \mid f$. Megjegyezzük, hogy ha $R[x]$ alaptételes, akkor f és g kanonikus alakját felírva a kitüntetett közös osztó képletéből (3.1.11. Gyakorlat (3)) is ezt az eredményt kapjuk.

3.2.17. Ezek azok a részhalmazok, amelyek egy adott szám összes többszöröséből állnak. Egy d szám többszöröseinek halmaza nyilván zárt az összeadásra, és nyilván minden elemének minden többszörösét is tartalmazza.

Megfordítva, legyen $I \subseteq \mathbb{Z}$ ilyen tulajdonságú, nem üres halmaz. Ha I csak a nullából áll, akkor ez a nulla összes többszöröseinek halmaza. Ha nem, akkor van I-ben pozitív szám is, hiszen ha $-k \in I$, akkor $k \in I$ (mert k többszöröse $-k$-nak). Legyen d az I halmaz legkisebb pozitív eleme. Megmutatjuk, hogy I pontosan a d többszöröseiből áll. Az a feltételből nyilvánvaló, hogy d többesei benne vannak I-ben. Legyen most $n \in I$, és osszuk el n-et maradékosan d-vel:

$$n = dq + r\,,$$

ahol $0 \leq r < d$. Innen $r = n + (-q)d \in I$, hiszen I zárt az összeadásra. Mivel I-ben nincs d-nél kisebb pozitív szám, $r = 0$, és így $d \mid n$. Vagyis I tényleg d többszöröseiből áll.

A 1.5.4. Tétel bizonyításában egy z komplex szám jó kitevőinek halmazát vizsgáltuk. Nyilvánvaló, hogy ez az I halmaz a feladatban leírt tulajdonságú: ha $z^n = 1 = z^m$, akkor $z^{n+m} = 1$, és minden k egészre $z^{nk} = 1$. Tehát az I halmaz egy pozitív d többszöröseiből áll (és ez a d pontosan a z rendje lesz).

3.3. Gyökök és irreducibilitás.

3.3.1. A polinomot (hacsak nem a nullapolinomról van szó) felírhatjuk $g(x)x^k$ alakban, ahol g konstans tagja már nem nulla, és a g polinomra alkalmazhatjuk a tesztet. Az eredeti polinomnak g gyökei mellett még a nulla lesz gyöke.

3.3.2. Az első három polinom esetében úgy érdemes eljárni, hogy a polinomot $\mathbb{C}$ felett gyöktényezők szorzatára bontjuk, majd a nem valós gyökökhöz tartozó gyöktényezőket párosítjuk a konjugáltjukkal. A gyökvonást trigonometrikus alakban célszerű elvégezni. A módszert részletesen bemutattuk a 2.5.5. Gyakorlat megoldásában, ezért most csak az eredményeket közöljük:

$$x^4 - 1 = (x-1)(x+1)(x^2+1)\,,$$
$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)\,,$$
$$x^4 + 9 = (x^2 - \sqrt{6}x + 3)(x^2 + \sqrt{6}x + 3)\,.$$

Az $x^6 - 4x^3 + 3 = 0$ egyenletet az $y = x^3$ helyettesítéssel oldhatjuk meg, ez y-ban másodfokú egyenletre vezet, melynek gyökei 1 és 3. Tehát $x^6 - 4x^3 + 3 = (x^3-1)(x^3-3)$. Mindkét tényezőnek egyetlen valós gyöke van, tehát az eredmény:

$$x^6 - 4x^3 + 3 = (x-1)(x^2+x+1)(x - \sqrt[3]{3})(x^2 + \sqrt[3]{3}x + \sqrt[3]{9})\,.$$

3.3.3. Figyelnünk kell arra, hogy a felsorolt négy gyűrű felett nemcsak az irreducibilis polinomok mások, hanem az egységek is. Ennek megfelelően egy $\mathbb{C}$ feletti felbontás

$$(6x + 6\sqrt{2})(x - \sqrt{2})(x+i)(x-i)$$

(a 6 itt egység, tehát külön tényezőként nem szerepelhet, de bármelyik másik irreducibilis tényezőbe is beolvaszthattuk volna). Amikor $\mathbb{R}$ fölött dolgozunk, akkor x^2+1 már irreducibilis lesz, mert másodfokú, és nincsen valós gyöke. Így az $\mathbb{R}$ fölött jó felbontások például a következők:

$$(2x + 2\sqrt{2})(3x - 3\sqrt{2})(x^2+1) = (x + \sqrt{2})(x - \sqrt{2})(6x^2+6)\,.$$

A $\mathbb{Q}$ fölött az $x^2 - 2$ is irreducibilis, hiszen másodfokú, és nincs racionális gyöke, és így a következőt kapjuk:

$$(x^2-2)(6x^2+6)\,.$$

Végül $\mathbb{Z}$ fölött az egységek csak a ± 1, tehát 2 és 3 is felbonthatatlan polinomok. Az x^2-2 és x^2+1 polinomokat $\mathbb{Z}$ fölött nem lehet alacsonyabb fokúak szorzatára bontani, hiszen láttuk, hogy $\mathbb{Q}$ fölött is irreducibilisek. De nem lehet őket $\mathbb{Z}$ fölött egy nulladfokú (azaz konstans polinom) és egy másodfokú polinom szorzatára sem nemtriviálisan felbontani, hiszen semmilyen ± 1-től különböző konstans nem emelhető ki belőlük. Ezért a $\mathbb{Z}$ feletti felbontás:

$$2 \cdot 3 \cdot (x^2-2) \cdot (x^2+1)\,.$$

Ezt csak úgy variálhatjuk, hogy néhány (páros sok) tényezőt -1-gyel beszorzunk.

3.3.4. A 3.3.6. Lemma miatt a polinomnak $-i$ is hatszoros gyöke, és ezért

$$(x-i)^6(x+i)^6 g(x) = (x^2+1)^6 g(x)$$

alakban írható. Mivel $(x^2+1)^6$ valós együtthatós, g is az (a 3.2.2. Állítás miatt). Ez a szorzat akkor lesz tizenkettedfokú, ha g konstans. Tehát a keresett polinomok pontosan az $r(x^2+1)^6$ polinomok, ahol $r \neq 0$ valós szám.

3.3.5. A racionális gyöktesztet alkalmazzuk (3.3.9. Tétel). Ha p/q racionális gyöke ennek a polinomnak, ahol p és q relatív prím egészek, akkor $p \mid 5$ és $q \mid 2$. A lehetséges gyökök tehát

$$1,\ \ -1,\ \ 1/2,\ \ -1/2,\ \ 5,\ \ -5,\ \ 5/2,\ \ -5/2\,.$$

Ezeket végig kell próbálgatni. Az rögtön látszik, hogy pozitív gyök nem lehet, a negatívakat behelyettesítve azt kapjuk, hogy csak a -1 lesz racionális gyök. A gyöktényezőt (például a Horner-elrendezéssel) kiemelve

$$2x^3+3x+5 = (x+1)(2x^2-2x+5)$$

adódik. A $2x^2-2x+5$ polinomnak racionális gyöke más, mint -1, nem lehet, mert az gyöke lenne az eredeti polinomnak is. Látjuk, hogy -1 nem gyök, és mivel ez másodfokú polinom, irreducibilis $\mathbb{Q}$ fölött (miként az elsőfokú $x+1$ is).

3.3.6. Ha $c > 0$, akkor $\mathbb{C}$ fölött gyöktényezős alakra bontva, a 3.3.2. Gyakorlat mintájára

$$x^4+c = (x^2-\sqrt{2}\sqrt[4]{c}x+\sqrt{c})(x^2+\sqrt{2}\sqrt[4]{c}x+\sqrt{c})\,.$$

Már megvizsgáltuk azt az esetet (a 3.3.10. Példában), amikor $c = 36$. Ugyanez a gondolatmenet általában is azt adja, hogy az x^4+c polinom akkor és csak akkor lesz reducibilis $\mathbb{Q}$ fölött, ha $\sqrt{2}\sqrt[4]{c}$ és $\sqrt{c}$ is racionális szám, és ebben az esetben a fenti két másodfokú tényező $\mathbb{Q}$, sőt $\mathbb{R}$ fölött is irreducibilis, hiszen másodfokúak, és nincs valós gyökük (mert x^4+c-nek sincs). Megjegyezzük, hogy ha $\sqrt{2}\sqrt[4]{c}$ racionális szám, akkor a négyzete, azaz $2\sqrt{c}$ is az, és így $\sqrt{c}$ is. Könnyű meggondolni, hogy (egész c esetén) $\sqrt{2}\sqrt[4]{c}$ akkor és csak akkor racionális, ha c kanonikus alakjában minden $p > 2$ prím kitevője néggyel osztható, a 2 kitevője pedig $4k-2$ alakú.

Ha $c < 0$, akkor legyen $d = -c > 0$. Ebben az esetben, ismét a $\mathbb{C}$ feletti gyöktényezős alakból kiindulva, az $\mathbb{R}$ fölötti felbontás

$$x^4-d = (x-\sqrt[4]{d})(x+\sqrt[4]{d})(x^2+\sqrt{d})\,.$$

Belátjuk, hogy x^4-d akkor és csak akkor irreducibilis $\mathbb{Q}$ fölött, ha $\sqrt{d}$ irracionális szám. Valóban, x^4-d-nek akkor és csak akkor van racionális gyöke, ha $\sqrt[4]{d}$ racionális szám (ekkor a négyzete, azaz $\sqrt{d}$ is racionális). Ha nincs racionális gyöke, akkor csak két másodfokú, racionális együtthatós polinom szorzatára bomolhat. Ezek közül valamelyiknek gyöke lesz $i\sqrt[4]{d}$, és akkor a konjugáltja is, tehát ez a tényező $q(x^2+\sqrt{d})$ alakú, ahol $q \in \mathbb{C}$. Mivel $q(x^2+\sqrt{d}) \in \mathbb{Q}[x]$, ezért q és $q\sqrt{d}$ is racionális, tehát $\sqrt{d}$ is az. Megfordítva, ha $\sqrt{d}$ racionális, akkor $(x^2-\sqrt{d})(x^2+\sqrt{d})$ jó felbontás.

3.3.7. Test fölött konstans polinom sosem, elsőfokú polinom mindig irreducibilis. A $\mathbb{Z}_2$ fölött összesen két elsőfokú polinom van: x és $x+1$. Mivel $\mathbb{Z}_2$ test, ezek irreducibilisek.

Test fölött egy másod- vagy harmadfokú polinom akkor és csak akkor irreducibilis, ha nincs az adott testben gyöke. A $\mathbb{Z}_2$ elemei 0 és 1, ezek nem szabad tehát, hogy gyökök legyenek. A négy $\mathbb{Z}_2$ fölötti másodfokú polinom közül x^2-nek és x^2+x-nek gyöke a nulla, x^2+1-nek pedig az 1. Tehát az egyetlen másodfokú irreducibilis polinom az x^2+x+1.

Érdemes itt egy pillanatra megállni, és megvizsgálni, hogyan is bomlik fel az x^2+1 polinom alacsonyabb fokúak szorzatára. Mivel az x^2+1-nek az 1 gyöke, az $x-1$ gyöktényező kiemelhető. Már itt problémánk lehet: polinom ez? Hiszen egy $\mathbb{Z}_2[x]$-beli polinomnak minden együtthatója 0 és 1 lehet csak. De tudjuk, hogy a -1 jelentése az 1 ellentettje, vagyis $\mathbb{Z}_2$-ben $-1=1$ (más szóval, pongyolán fogalmazva: „az előjelek nem számítanak"). Vagyis $x-1$ helyett $x+1$-et is írhatunk. A kiemelést például a Horner-eljárással végezve

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

adódik. Ezt beszorzással is ellenőrizhetjük:

$$(x+1)(x+1)=x^2+x+x+1=x^2+(1+_2 1)x+1=x^2+0\cdot x+1=x^2+1\,.$$

(Ha valaki e számolást nem érzi egészen precíznek, az használja a szorzás elvégzésekor a szorzatpolinom együtthatóját megadó (2.1.1) képletet a 43. oldalon.) Ugyanígy az is kijön, hogy tetszőleges $f, g \in \mathbb{Z}_2[x]$ polinomokra

$$(f+g)^2=f^2+g^2\,,$$

hiszen $fg+gf=(1+_2 1)fg=0$. Vagyis $\mathbb{Z}_2$ *fölött tagonként lehet négyzetre emelni.* Ezt a hasznos tulajdonságot sokszor kiaknázzuk majd.

Mivel a harmadfokú irreducibilisek is azok, amelyeknek nincs gyöke, ezeket is könnyen felsorolhatjuk. A polinom főtagja x^3, konstans tagja, mivel a 0 nem gyök, csakis 1 lehet. Végül a polinom (nem nulla) tagjainak száma páratlan, különben az 1 gyöke lenne. Így $\mathbb{Z}_2$ fölött két harmadfokú irreducibilis polinom van:

$$x^3+x+1 \qquad \text{és} \qquad x^3+x^2+1\,.$$

A negyedfokú irreducibilis polinomok megkeresése már nem ilyen egyszerű. Persze ezeknek sem lehet $\mathbb{Z}_2$-ben gyöke. Az olyan polinomokat, amelyeknek nincs gyöke, a harmadfokú esethez hasonlóan felsorolhatjuk:

$$x^4+x+1\,, \qquad x^4+x^2+1\,, \qquad x^4+x^3+1\,, \qquad x^4+x^3+x^2+x+1\,.$$

Ezek azonban nem feltétlenül irreducibilisek $\mathbb{Z}_2$ fölött. Tudjuk, hogy a gyök létezése elsőfokú tényezőt jelent, vagyis ha a felsorolt polinomok valamelyike reducibilis, akkor csakis két másodfokú f és g polinom szorzatára bomolhat. Itt f-nek és g-nek nincs gyöke $\mathbb{Z}_2$-ben (hiszen szorzatuknak sincs), és ezért ők irreducibilis, másodfokú polinomok. De már felsoroltuk a másodfokú irreducibilis polinomokat, ezek szerint f és g is csak x^2+x+1 lehet. Szorzatuk,

$$f(x)g(x)=(x^2+x+1)^2=x^4+x^2+1$$

(a négyzetre emelést természetesen tagonként végeztük). Tehát a felsorolt négy polinomból ez az egy nem irreducibilis, a másik három igen.

3.3.8. Ha $0 < i < p$, akkor a

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{1\cdot 2\cdot \dots \cdot i}$$

binomiális együttható p-vel osztható, hiszen a számláló osztható p-vel, a nevező viszont nem (mert p prím, de a nevező egyik tényezőjének sem osztója). Ha egy n szám osztható p-vel, azaz $n = pm$, akkor tetszőleges $r \in R$ elemre

$$nr = (mp)r = m(pr) = m \cdot 0 = 0$$

(felhasználtuk a hatványozásnak a 2.2.8. Gyakorlat (3) pontjában leírt tulajdonságát a többszörös fogalmára átalakítva). A binomiális tételből azt kapjuk, hogy

$$(r+s)^p = r^p + \binom{p}{1} r^{p-1}s + \dots + \binom{p}{p-1} r s^{p-1} + s^p\,.$$

A szereplő binomiális együtthatók a fentiek szerint p-vel oszthatók, és így az összegből csak $r^p + s^p$ marad meg, a többi tag nulla lesz. (Itt természetesen a binomiális tételnek az általános gyűrűkre vonatkozó változatát alkalmaztuk, amelyet a 2.2.17. Gyakorlatban fogalmaztunk meg).

A kis Fermat Tétel bizonyításához (modulo p számolva) elég azt megmutatni, hogy $b \in \mathbb{Z}_p$ esetén $b^p = b$. Emeljük p-edik hatványra a b darab 1-esből álló összeget:

$$(1+1+\dots+1)^p = 1^p + 1^p + \dots + 1^p\,.$$

A baloldalon b^p áll, a jobboldalon pedig b.

Végül ha $f(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}_p[x]$, akkor, mivel tagonként lehet p-edik hatványra emelni, $f(x)^p = a_0^p + \dots + a_n^p (x^p)^n$. De $a_i \in \mathbb{Z}_p$ miatt $a_i^p = a_i$, és így ez tényleg $f(x^p)$.

3.3.9. A $\mathbb{Z}_2$ fölötti irreducibilitás vizsgálatához érdemes átfutni a 3.3.7. Gyakorlat megoldását, amelyben felsoroltuk a legfeljebb negyedfokú irreducibilis polinomokat, és amelyből kiderül, hogy itt tagonként lehet négyzetre emelni. Ezeket az eredményeket az alábbiakban felhasználjuk.

$x^8 + x^2 + 1 = (x^4 + x + 1)^2$ (tagonkénti „négyzetgyökvonással”), vagyis ez egy irreducibilis polinom négyzete.

$x^5 + x + 1$-nek nincs $\mathbb{Z}_2$-ben gyöke (sem a 0, sem az 1 nem gyök), ezért nincs elsőfokú tényezője. Ha felbomlik, akkor tehát csak egy másod- és egy harmadfokú irreducibilis szorzata lehet. Az egyetlen másodfokú irreducibilis polinom az $x^2 + x + 1$, ezzel osztva a maradék nulla lesz, és $x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1)$ adódik.

$x^5 + x^3 + 1$-nek nincs $\mathbb{Z}_2$-ben gyöke, és $x^2 + x + 1$-gyel sem osztható, vagyis irreducibilis.

$x^5 + x^4 + x^3 + 1$-nek gyöke az 1, a gyöktényezőt (például a Horner-elrendezéssel) kiemelve az $(x+1)(x^4 + x^2 + x + 1)$ felbontás adódik. Ez utóbbi tényezőnek ismét gyöke az 1, vagyis $x^5 + x^4 + x^3 + 1 = (x+1)^2(x^3 + x^2 + 1)$ a felbontás irreducibilisek szorzatára.

A $\mathbb{Z}_{17}$ fölött a támpontunk a 3.3.8. Feladat, mely szerint $\mathbb{Z}_{17}[x]$-ben tagonként lehet 17-edik hatványra emelni.

x^2+1 másodfokú, tehát csak a gyökeit kell ellenőrizni, vagyis -1-ből, azaz 16-ból kell négyzetgyököt vonni. Az eredmény nyilván ± 4 ezért $x^2+1=(x+4)(x-4)=(x+4)(x+13)$.

x^4+1 ezek szerint $(x^2+4)(x^2-4)$ alakban írható. A tényezők másodfokúak, tehát ismét a gyökeiket kell megvizsgálni. Nyilván $x^2-4=(x+2)(x-2)$. Másfelől a -1 négyzetgyökei ± 4, tehát -4 négyzetgyökei ± 8. Így $x^4+1=(x+2)(x-2)(x+8)(x-8)$.

x^8+1 az előzőek szerint $(x^2+2)(x^2-2)(x^2+8)(x^2-8)$. Itt is mindegyik négyzetgyökvonás elvégezhető: $x^8+1=(x+7)(x-7)(x+6)(x-6)(x+3)(x-3)(x+5)(x-5)$.

$x^{17}+1=(x+1)^{17}$, tagonkénti 17-edik hatványra emeléssel.

$x^{17}+2=x^{17}+1+1$. Tagonkénti 17-edik „gyökvonással” ez $(x+2)^{17}$. A kis Fermat Tétel miatt igazából $x^{17}+c=(x+c)^{17}$ minden $c\in\mathbb{Z}_{17}$ esetén.

3.3.10. Ez is hasonló a 3.3.10. Példa megoldásához, azonban van benne egy extra csavar. Az x^4-10x^2+1 polinom négy gyöke $\pm\sqrt{2}\pm\sqrt{3}$, amit a legegyszerűbb úgy ellenőrizni, hogy az

$$(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$$

gyöktényezős felbontásban elvégezzük a beszorzást (ezt mindjárt meg is tesszük majd). Ez tehát az $\mathbb{R}$ feletti felbontás irreducibilisek szorzatára.

A racionális gyökteszt segítségével megállapíthatjuk, hogy az x^4-10x^2+1 polinomnak nincs racionális gyöke (ennél számolósabb közvetlenül kihozni, hogy $\pm\sqrt{2}\pm\sqrt{3}$ irracionális szám). Ha tehát ez a polinom nem lenne irreducibilis $\mathbb{Q}$ fölött, akkor két másodfokú, irreducibilis polinom szorzatára bomolhatna csak.

A 3.3.10. Példa megoldásában két konjugált komplex gyökpár szerepelt, és így egy másodfokú, valós együtthatós tényező gyökei konjugáltak voltak. Most azonban négy valós gyök van, és így elvileg bármely kettőből gyárthatnánk egy másodfokú, racionális együtthatós tényezőt. Nem tehetünk mást, mint hogy ezeket a gyöktényezőket minden lehetséges módon párosítjuk egymással, és elvégezzük a beszorzást. Összesen háromféle párosítás lehetséges. Mindhárom esetben ismét az $(a-b)(a+b)=a^2-b^2$ azonosság felhasználásával egyszerűsíthetjük a számolást. A három eredmény a következő lesz:

$$\begin{aligned}&(x^2-2\sqrt{2}x-1)(x^2+2\sqrt{2}x-1)=\\&=(x^2-2\sqrt{3}x+1)(x^2+2\sqrt{3}x+1)=\\&=(x^2-5-2\sqrt{6})(x^2-5+2\sqrt{6})\,.\end{aligned}$$

Mindhárom felbontásban normált, de nem racionális együtthatós polinomok szerepelnek, és így a 3.3.10. Példa gondolatmenete szerint egyik sem ad $\mathbb{Q}$ feletti felbontást. Beláttuk tehát, hogy x^4-10x^2+1 irreducibilis $\mathbb{Q}$ fölött.

Ha $\mathbb{Z}_5$ felett dolgozunk, akkor $\sqrt{6}$ értéke 1 lesz, és így a fenti felbontások közül a harmadik működni fog:

$$x^4 - 10x^2 + 1 = (x^2 - 5 - 2)(x^2 - 5 + 2) = (x^2 - 2)(x^2 + 2)\,.$$

E két tényező már irreducibilis $\mathbb{Z}_5$ felett, hiszen másodfokúak, és $\mathbb{Z}_5$ elemeit végigpróbálhatva látjuk, hogy nincs gyökük. A $\mathbb{Z}_7$ fölött a ±1, ±2, ±3 számokat négyzetre emelve látjuk, hogy a 2-ből vonható négyzetgyök (az eredmény ±3), a 3-ból viszont nem. Ezért ebben az esetben a fenti első felbontás fog működni:

$$x^4 - 10x^2 + 1 = (x^2 - 6x - 1)(x^2 + 6x - 1)\,.$$

E két tényező ismét irreducibilis. Végül $\mathbb{Z}_{11}$ fölött a 3-nak lesz négyzetgyöke (a ±5), és így itt a fenti második felbontás adja a megoldást:

$$x^4 - 10x^2 + 1 = (x^2 - 10x + 1)(x^2 + 10x + 1)\,.$$

Aki járatos számelméletből a kvadratikus maradékok elméletében (azaz tud bánni az úgynevezett Legendre-szimbólumokkal), az könnyen végiggondolhatja, hogy tetszőleges $p > 3$ prím esetén a 2, 3, 6 számok közül mindig pontosan egy lesz, amelyből négyzetgyök vonható modulo p. Emiatt a fenti három felbontás egyike mindig működni fog, és a kapott két másodfokú tényezőnek sosem lesz gyöke. Vagyis minden ilyen p-re az $x^4 - 10x^2 + 1 \in \mathbb{Z}_p[x]$ polinom két másodfokú irreducibilis szorzatára bomlik.

Ez azért érdekes, mert a későbbiekben látni fogjuk, hogy egy polinom modulo p vizsgálata sokszor segít az irreducibilitás eldöntésében. A 107. oldalon található táblázatban szerepel több ilyen módszer is, de a fenti polinom irreducibilitását egyik sem bizonyítja (például az eddigiek alapján könnyű belátni, hogy $x^4 - 10x^2 + 1$ semmilyen eltoltjára sem alkalmazható az úgynevezett Schönemann-Eisenstein-kritérium).

3.4. Egész együtthatós polinomok.

3.4.1. Legyen p felbonthatatlan egész szám. Ekkor p nem nulla és nem egység $\mathbb{Z}$-ben (azaz nem ±1). Mivel $\mathbb{Z}[x]$ egységei is ±1 (3.1.7. Gyakorlat), ezért p nem nulla és nem egység $\mathbb{Z}[x]$-ben sem. Meg kell még mutatni, hogy a $\mathbb{Z}[x]$-beli felbontásai is triviálisak. Ha $p = fg$, ahol $f, g \in \mathbb{Z}[x]$, akkor f és g fokainak összege nulla, ezért f és g is konstans polinom. Így a $\mathbb{Z}[x]$-beli és a $\mathbb{Z}$-beli felbontások ugyanazok. Mivel az egységek is ugyanazok ebben a két gyűrűben, a triviális felbontások is ugyanazok lesznek.

3.4.2. Azt a 3.4.4. Következmény bizonyításában láttuk, hogy minden racionális együtthatós polinom felírható rf alakban, ahol r racionális szám, és f primitív, egész együtthatós polinom. Tegyük fel, hogy $rf = sh$, ahol s is racionális szám, és h is primitív, egész együtthatós polinom. Ekkor $h = (r/s)f$, vagyis f osztója h-nak $\mathbb{Q}[x]$-ben. A 3.4.4. Következmény miatt $f \mid h$ teljesül $\mathbb{Z}[x]$-ben is. A szerepeket felcserélve a $h \mid f$ oszthatóságot kapjuk, szintén $\mathbb{Z}[x]$-ben. Tehát f és h tényleg asszociáltak $\mathbb{Z}[x]$-ben. Ebből az is következik, hogy r és s vagy egyenlők, vagy egymás ellentettjei.

3.4.3. $30x^3 - 30 = 2 \cdot 3 \cdot 5 \cdot (x-1) \cdot (x^2 + x + 1)$. Az itt szereplő tényezők közül 2, 3, 5 irreducibilis $\mathbb{Z}$ fölött, mert $\mathbb{Z}$-beli prímek, $x - 1$ mert primitív, és $\mathbb{Q}$ fölött irreducibilis (lévén elsőfokú), végül $x^2 + x + 1$ szintén, azért, mert primitív és $\mathbb{Q}$ fölött irreducibilis (hiszen másodfokú, és nincs racionális gyöke).

3.4.4. A 3.1.7. Gyakorlat szerint R és $R[x]$ egységei ugyanazok. Mivel R nullosztómentes, egy nem nulla konstans R-beli polinom minden felbontása csakis nulladfokú, azaz konstans polinomok szorzatára történhet. Egy ilyen felbontás akkor és csak akkor triviális R-ben, ha $R[x]$-ben az (mert ugyanazok az egységek).

Ezek az észrevételek először is azt mutatják, hogy egy konstans polinom akkor és csak akkor irreducibilis R-ben, amikor $R[x]$-ben. Ha tehát R egy elemét $R[x]$-ben irreducibilisek szorzatára bontjuk, akkor ez egyben egy R-ben irreducibilisek szorzatára történő felbontás is lesz. Így R-ben minden nem nulla és nem egység elem irreducibilisek szorzatára bontható. Mivel az egységek ugyanazok R-ben és $R[x]$-ben, két R-beli elem akkor és csak akkor asszociált R-ben, ha $R[x]$-ben az. Emiatt a felbontás $R[x]$-beli egyértelműségéből az R-beli egyértelműség adódik.

3.4.5. Legyen f nem nulla és nem egység polinom $\mathbb{Z}[x]$-ben. Ha f konstans, akkor a $\mathbb{Z}$-beli irreducibilisekre való felbontása megfelelő lesz. Ha nem konstans, akkor felírható $\mathbb{Q}[x]$-beli irreducibilisek szorzataként. A második Gauss-lemma (3.4.5. Lemma) miatt feltehető, hogy ezek a tényezők egész együtthatósak (és továbbra is irreducibilisek, hiszen ezen egy racionális számmal való szorzás nem változtat). Tehát elég belátni, hogy egy egész együtthatós, $\mathbb{Q}[x]$-ben irreducibilis g polinom felbontható $\mathbb{Z}[x]$-ben irreducibilisek szorzatára.

Írjuk fel a g polinomot nh alakban, ahol n egész szám, és h primitív, egész együtthatós polinom. Az n-et felbonthatjuk a $\mathbb{Z}$-beli alaptétel szerint, a h pedig irreducibilis lesz $\mathbb{Z}$ fölött, mert primitív, és $\mathbb{Q}$ fölött irreducibilis.

3.4.6. Legyen $f = mf_0$ és $g = kg_0$, ahol f_0 és g_0 primitív polinomok. Az m és k egész számokat $\mathbb{Z}$-ben, az f_0 és g_0 polinomokat $\mathbb{Z}[x]$-ben felbonthatjuk irreducibilisek szorzatára, ez utóbbiak tényezői is primitív polinomok lesznek. A 3.1.11. Gyakorlatban láttuk, hogy a kanonikus alakból hogyan lehet megkapni a kitüntetett közös osztót. Ezt alkalmazva adódik, hogy f és g kitüntetett közös osztója nh lesz, ahol n az m és k egész számok legnagyobb közös osztója, h pedig (az első Gauss-lemma első következménye miatt) egy primitív polinom (az f_0 és a g_0 közös irreducibilis tényezőinek a szorzata). Mindezt $\mathbb{Q}$ fölött nézve a konstans szorzók nem számítanak, tehát itt h lesz a kitüntetett közös osztó. Ezért kapható meg h és n is a leírt módon (itt felhasználtuk, hogy az nh felbontás lényegében egyértelmű a 3.4.2. Gyakorlat miatt).

A $\mathbb{C}[x, y]$-ban is működik ugyanez, csak nem racionális törtekkel, hanem racionális törtfüggvényekkel kell számolni. Vagyis $\mathbb{C}[x, y]$ elemeit x polinomjának képzelve elvégezhetjük az euklideszi algoritmust, az eljárásban fellépő polinomok együtthatói $p(y)/q(y)$ alakú törtek lesznek, ahol $p, q \in \mathbb{C}[y]$. Az f és g együtthatóit is $\mathbb{C}[y]$-beli polinomoknak képzeljük, és így keressük meg a kitüntetett közös osztójukat. Általában ha R alaptételes gyűrű,

akkor $R[x]$-ben működik a leírt eljárás, feltéve, hogy R elemeinek már ki tudjuk számítani a kitüntetett közös osztóját.

3.4.7. Ha T test, akkor minden nem nulla eleme egység. Így nincs benne sem irreducibilis, sem prím, de az igaz, hogy minden nullától és egységtől különböző eleme egyértelműen felbontható irreducibilisek szorzatára. (Aki nem hiszi, hozzon ellenpéldát: mutasson egy olyan nem nulla és nem egység elemet T-ben, amely nem bontható fel, vagy a felbontása nem egyértelmű. Senki nem tud ilyen ellenpéldát hozni, mert már nem nulla és nem egység elemet sem fog találni egy testben.)

Annak bizonyításában, hogy alaptételes gyűrű feletti polinomgyűrű is alaptételes, kihasználtuk, hogy test fölötti polinomgyűrű alaptételes (a $\mathbb{Q}[x]$-ben használtuk az alaptételt, amikor $\mathbb{Z}[x]$-et vizsgáltuk), tehát erre nem kaptunk új bizonyítást.

3.5. Irreducibilitás a racionális számtest fölött.

3.5.1. Az állítás közvetlen számolással is igazolható (egy $rx^n = fg$ felbontás tényezőiben a legmagasabb és legalacsonyabb fokú tagok vizsgálatával, a 3.1.25. Gyakorlat mintájára). Elegánsabb azonban a következő gondolatmenet. A $T[x]$ alaptételes gyűrű, amelyben az x irreducibilis polinom (hiszen elsőfokú). Tehát rx^n kanonikus alakban van, és így osztói az x legfeljebb n-edik hatványainak asszociáltjai (lásd 3.1.11. Gyakorlat, (2) pont).

3.5.2. Tegyük fel, hogy az $f(x) = a_0 + \cdots + a_n x^n$ polinom és a p prímszám teljesítik a feltételeket, de f mégsem irreducibilis $\mathbb{Q}$ fölött, vagyis az f-nél alacsonyabb fokú, racionális együtthatós $g(x) = b_0 + \cdots + b_k x^k$ és $h(x) = c_0 + \cdots + c_\ell x^\ell$ polinomok szorzatára bontható (így $k, \ell < n$). A második Gauss-lemma (3.4.5. Lemma) miatt feltehetjük, hogy g és h egész együtthatós.

Mivel $a_n = b_k c_\ell$, a b_k és c_ℓ egészek egyike sem osztható p-vel. Ugyanakkor $a_0 = b_0 c_0$, és mivel a_0 osztható p-vel, de p^2-tel nem, a b_0 és c_0 számok közül pontosan az egyik osztható p-vel. Szimmetriaokokból (g és h esetleges cseréjével) feltehetjük, hogy ez a b_0.

Haladjunk végig a g polinom együtthatóin a b_0-tól kezdve addig, amíg p-vel osztható számot látunk. Legyen i az első olyan index, amelyre b_i nem osztható p-vel. Ilyen i van, hiszen b_0 osztható p-vel, de b_k nem, és persze $0 < i \leq k$. Ekkor az $f = gh$ polinomban az

$$a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_{i-1} c_1 + b_i c_0$$

együttható nem osztható p-vel, mert az összeg mindegyik tagja osztható vele, kivéve az utolsó tagot. A feltétel szerint f együtthatói oszthatók p-vel, kivéve a_n-et. Ezért $i = n$, azaz $i \leq k$ miatt $k \geq n$. Ez ellentmond a $k < n$ feltételnek.

3.5.3. A felsorolt állítások közül csak (4) és (6) igaz!

(1) Ellenpélda: $x^2 + 1$ mod 2 véve.
(2) Ellenpélda: $2x^2 + x$ mod 2 véve.
(3) Ellenpélda: $3x$ mod 5 véve.
(4) Ez az állítás igaz, és a jelenség már a Schönemann-Eisenstein kritérium bizonyításában is előjött. Tegyük fel, hogy f reducibilis, ekkor a második Gauss-lemma miatt felbontható a nála alacsonyabb fokú, egész együtthatós g és h polinomok szorzatára. Amikor egy polinomot mod p veszünk, akkor a fokszáma nem nőhet (de csökkenhet, ha a főegyütthatója p-vel osztható). Tehát ha az $f = gh$ felbontást mod p vesszük, akkor

$$\mathrm{gr}(\overline{g}) \le \mathrm{gr}(g) < \mathrm{gr}(f) = \mathrm{gr}(\overline{f})\,,$$

és ugyanígy $\mathrm{gr}(\overline{h}) < \mathrm{gr}(\overline{f})$. Tehát mod p is nemtriviális felbontást kapunk.
(5) Ellenpélda: $2x + 1$ mod 2 véve, $k = 1$.
(6) Ez igaz, és a bizonyítás ugyanaz, mint a (4) pontban.

3.5.4. Ha az f polinomot szorzattá lehet bontani: $f = gh$, akkor az összes eltoltjait is ugyanúgy szorzattá bonthatjuk, hiszen $f(x+c) = g(x+c)h(x+c)$ is teljesül. Megfordítva, ha $f(x + c)$ felbontható, akkor az $x \to x - c$ helyettesítéssel f egy felbontását kapjuk.

Általában egy T test fölött az $x \to ax + b$ helyettesítésről is ugyanezt mondhatjuk el. Ennek is van „inverze”: az $f(ax + b)$ polinom egy felbontásából az x helyébe $x/a - b/a$-t írva az f egy felbontását kapjuk. Fontos megjegyezni, hogy eközben a szereplő polinomok foka nem változik, és így nemtriviális felbontásból mindig nemtriviális felbontás adódik.

Az állítás azon múlik, hogy $f(x) \to f(ax + b)$ a $T[x]$ polinomgyűrűnek önmagára menő, kölcsönösen egyértelmű, művelettartó leképezése (azaz izomorfizmusa). Ez a megközelítés azért kényelmesebb a fentinél, mert nem kell azzal foglalkoznunk, hogy a felbontások triviálisak-e! Csak ennyit kell mondanunk: az irreducibilis elem fogalmát a gyűrű műveletei segítségével definiáltuk, tehát izomorfizmusnál irreducibilis elem képe irreducibilis lesz.

Ezen a módon azt is láthatjuk, hogy ha nem test fölött vagyunk, hanem például $\mathbb{Z}[x]$-ben, akkor az „invertálható” helyettesítések, például az $x \to x + c$, megőrzik az irreducibilitást.

3.5.5. Az $f(x) = 1 + x + \cdots + x^{p-1}$ polinomba $x + 1$-et helyettesítve a főegyütthatója nem változik, továbbra is 1 marad. Az $f(x + 1)$ konstans tagját az $x = 0$ helyettesítéssel kaphatjuk meg, látjuk, hogy ez $f(1) = p$, ami p-vel osztható, de p^2-tel nem. Azt kell még belátni, hogy az $f(x + 1)$ polinom összes nem fő együtthatója p-vel osztható, vagyis hogy ezt a polinomot mod p véve x^{p-1} adódik. Ezért áttérünk $\mathbb{Z}_p[x]$-re.

Az ismert azonosság (vagy a mértani sor összegképlete) miatt

$$1 + (x + 1) + \cdots + (x + 1)^{p-1} = \frac{(x + 1)^p - 1}{(x + 1) - 1}\,.$$

Mivel $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.8. Feladat), ez tovább így alakítható:

$$\frac{(x+1)^p-1}{(x+1)-1}=\frac{x^p+1^p-1}{x}=x^{p-1}\,.$$

Így az állítást beláttuk.

3.5.6. Tegyük fel, hogy $6x^4+3x+1=f(x)g(x)$, ahol f és g legfeljebb harmadfokú, nem konstans polinomok; a második Gauss-lemma miatt feltehető, hogy egész együtthatósak. Vegyük ezt a felbontást modulo 3. Ekkor a baloldal a konstans 1 polinom lesz. Mivel $\mathbb{Z}_3$ nullosztómentes, az f és g is nem nulla konstans polinommá válik mod 3 véve. Egyik sem volt konstans eredetileg, tehát mindkettő főegyütthatója hárommal osztható kell, hogy legyen. De akkor szorzatuk főegyütthatója osztható kilenccel, ami nem igaz: ez a főegyüttható ugyanis 6.

3.5.7. Az előző gyakorlat megoldása szó szerint elmondható. Az f-et mod p véve konstans polinomot kapunk, mert minden együtthatója p-vel osztható. Ez a konstans nem nulla, mert az f konstans tagja nem osztható p-vel. Az előző gyakorlat gondolatmenete szerint ekkor f főegyütthatója p^2-tel osztható lenne.

3.5.8. Mindkét állítás bizonyításának kulcsa a következő észrevétel:

$$x^n f(1/x)=x^n(a_n/x^n+\cdots+a_1/x+a_0)=a_n+\cdots+a_1x^{n-1}+a_0x^n=g(x)\,.$$

Innen azonnal látszik, hogy a g gyökei pont az f gyökeinek a reciprokai (a nulla egyik polinomnak sem gyöke, mert a_0 és a_n nem nulla). Ha $b\in T$ az f-nek k-szoros gyöke, és így $f(x)=(x-b)^k h(x)$, akkor

$$g(x)=x^n f(1/x)=x^k\big((1/x)-b\big)^k x^{n-k}h(1/x)=\big((1/b)-x\big)^k b^k x^{n-k}h(1/x)\,,$$

ahol $b^kx^{n-k}h(1/x)$ is polinom, mert h foka $n-k$. Ezért $1/b$ legalább k-szoros gyöke g-nek. Ha $1/b$ a g-nek ℓ-szeres gyöke, akkor tehát $\ell\geq k$. Mivel f és g szerepe szimmetrikus, ugyanígy adódik, hogy $k\geq\ell$, és így a két multiplicitás megegyezik.

Ha $f(x)=p(x)q(x)$, ahol $p\in T[x]$ foka $k<n$, és $q\in T[x]$ foka $\ell<n$, akkor

$$g(x)=x^k p(1/x)\cdot x^\ell q(1/x)$$

a g-nek lesz felbontása ugyanilyen fokú polinomok szorzatára, és így g is reducibilis. Az f és g szimmetriája miatt tehát ez a két polinom ugyanakkor irreducibilis.

3.5.9. A megoldás ugyanaz, mint az x^4+x^2+x+1 polinom esetében, mert annál a számolásnál az x^2-es tag együtthatójából kapott egyenletet nem használtuk ki. De most más megoldás is kínálkozik: ez a polinom $\mathbb{Z}_2$ fölött irreducibilis (3.3.7. Gyakorlat), és mivel a főegyütthatója páratlan, irreducibilis $\mathbb{Q}$ fölött is (lásd 3.5.3. Gyakorlat, (4) pont).

3.5.10. Csak olyan prímszámokat érdemes nézni, amelyek a polinom nem fő együtthatóinak közös osztói. Így az $x^{11} + 2x + 18$ esetében csak a $p = 2$ jön szóba, és ez meg is felel, mert a 18 is páros, de nem osztható $p^2 = 4$-gyel. Ezért ez a polinom irreducibilis $\mathbb{Q}$ fölött (és mivel primitív, $\mathbb{Z}$ fölött is). Az $x^{11} + 2x + 12$ polinomnál is csak a $p = 2$ jön szóba, de ez sem megfelelő, mert 4 osztója a konstans tagnak, azaz 12-nek. Erre a polinomra tehát nem alkalmazható a Schönemann-Eisenstein-kritérium. ***Ebből azonban nem következik, hogy a polinom reducibilis!*** Az irreducibilitást ezen a módon nem sikerült eldönteni, tehát egy másik módszerrel kell próbálkoznunk.

Ugyanígy folytatva látjuk, hogy $x^{11} + 12x + 5$ esetében sem alkalmazható a kritérium (most nincs is közös prímosztója a nem fő együtthatóknak). Az $x^{11} + n$ polinomra akkor és csak akkor alkalmazható a kritérium, ha az n szám kanonikus alakjában van olyan prím, ami az első kitevőn szerepel. Vagyis $n = 24$ megfelelő ($p = 3$), de $n = 72$ nem.

3.5.11. Komplex fölött pontosan az elsőfokú polinomok irreducibilisek, tehát a három felsorolt polinom egyike sem az. Valós fölött az elsőfokú polinomok mellett azok a másodfokúak irreducibilisek, amelyeknek nincs valós gyöke. Ezért $x^2 + x + 1$ irreducibilis, de $x^7 + x + 1$ és $x^2 - 2$ nem az.

Mivel $\mathbb{Z}$ fölött egy nem konstans polinom akkor irreducibilis, ha primitív, és irreducibilis $\mathbb{Q}$ fölött, $3x^7 + 6x - 18$ nem irreducibilis $\mathbb{Z}$ fölött. A többi (3)-beli polinom primitív, és így a feladatban felsorolt összes polinomot a $\mathbb{Q}$ fölötti irreducibilitás szempontjából kell megvizsgálni; a megoldás hátralévő részében az „irreducibilis” és „reducibilis” szavakat ebben az értelemben használjuk.

Noha körosztási polinomokról még nem volt szó, egy esetleges későbbi ismétlés kedvéért megjegyezzük, hogy az alábbiakban szereplő polinomok közül $\Phi_{32}(x) = x^{16} + 1$, $\Phi_{12}(x) = x^4 - x^2 + 1$ és $\Phi_8(x) = x^4 + 1$ körosztási polinomok, és így a 3.9.4. Tétel miatt (is) irreducibilisek.

$3x^7 - 6x^6 + 6x^2 + 3x - 2$: irreducibilis, fordított Schönemann-Eisenstein ($p = 3$).

$3x^7 + x^6 + 6x^2 + 2x - 2$: reducibilis, a -1 gyöke (ez a racionális gyökteszt segítségével található meg).

$3x^7 - 6x^6 + 6x^2 + 2x - 2$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^{16} + 1$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann-Eisenstein $p = 2$-re. Ennek kiszámítását a 3.5.5. Feladat mintájára érdemes elvégezni (lásd 3.9.18. Gyakorlat).

$x^{16} + 2$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^4 - 14x^2 + 9$: irreducibilis, a 3.3.10. Feladat módszerével. A gyökei $\pm\sqrt{2} \pm \sqrt{5}$.

$x^4 - x^2 + 1$: irreducibilis, a 3.3.6. Gyakorlat módszerével. A gyökei a tizenkettedik primitív egységgyökök, az $\mathbb{R}$ feletti felbontása $(x^2 - \sqrt{3}x + 1)(x^2 + \sqrt{3}x + 1)$.

$3x^7 + 6x - 18$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^5 + 4$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann-Eisenstein ($p = 5$).

$x^3 + 9$: irreducibilis, mert harmadfokú, és nincs racionális gyöke (az egyetlen valós gyöke a $-\sqrt[3]{9}$, irracionális szám).

$x^3 + 3$: irreducibilis, Schönemann-Eisenstein $p = 3$-ra.

$x^{10} - x^5 + 1$: reducibilis, $x^2 - x + 1$ osztója. Ezt úgy lehet megtalálni, hogy $y = x^5$ helyettesítéssel megkeressük a gyököket. Mivel $y^2 - y + 1 = 0$, az y a két primitív hatodik egységgyök, η_1 és η_2 egyike lesz, ezekből kell ötödik gyököt vonni. De $\eta_1^5 = \eta_2$ és $\eta_2^5 = \eta_1$, így $x^{10} - x^5 + 1$-nek is gyöke η_1 és η_2, tehát osztható $(x - \eta_1)(x - \eta_2) = x^2 - x + 1$-gyel.

$x^{10} + 10$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^4 + 25$: irreducibilis, a 3.3.6. Gyakorlat eredménye szerint.

$x^4 + 2$: irreducibilis, Schönemann-Eisenstein ($p = 2$).

$x^4 + 4x + 1$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann-Eisenstein ($p = 2$).

$x^4 - 2x + 1$: reducibilis, az 1 gyöke.

$2x^4 + 2x^2 + 1$: irreducibilis, fordított Schönemann-Eisenstein ($p = 2$).

$x^6 - 10x + 10$: irreducibilis, Schönemann-Eisenstein ($p = 5$).

$x^4 + x^3 + x^2 + 1$: irreducibilis, ez a 3.5.2. Példában szereplő polinomhoz tartozó reciprok polinom (lásd 3.5.8. Feladat).

$x^4 + 2x + 27$: irreducibilis, $x \to x + 1$ helyettesítés után Schönemann-Eisenstein ($p = 2$).

$x^6 + 1$: reducibilis, az ismert azonosság szerint $(x^2 + 1)(x^4 - x^2 + 1)$.

$x^3 + 7x - 3$: irreducibilis, mert harmadfokú, és a racionális gyökteszt miatt nincs racionális gyöke.

$x^4 + 3x^3 + x^2 + 1$: reducibilis, a -1 gyöke.

3.5.12. Legyen h többszöröse f-nek $\mathbb{Z}[x]$-ben. Megmutatjuk, hogy $f(x) \mid f\big(x + h(x)\big)$. Valóban, ha $f(x) = a_0 + \cdots + a_n x^n$, akkor

$$f\big(x + h(x)\big) - f(x) = (a_0 - a_0) + \cdots + a_n\big(x + h(x)\big)^n - a_n x^n .$$

Az $a - b \mid a^k - b^k$ összefüggés miatt $\big(x + h(x)\big)^k - x^k$ osztható $x + h(x) - x = h(x)$-szel, és így $f(x)$-szel is. Ezért $f(x) \mid f\big(x + h(x)\big) - f(x)$, ahonnan $f(x) \mid f\big(x + h(x)\big)$.

Ebből már láthatjuk, hogy a keresett f polinom nem létezik. Az f nem lehet konstans, mert akkor $f\big(g(x)\big)$ is az, és így nem irreducibilis $\mathbb{Q}$ fölött. Ha viszont f nem konstans, akkor az előző bekezdésben bizonyított állítás $h(x) = xf(x)$ és $g(x) = x + h(x)$ választással ellentmondásra vezet: ekkor $f\big(g(x)\big) = f\big(x + h(x)\big)$ osztható f-fel, és így csak akkor lehetne irreducibilis, ha f konstansszorosa lenne, de a foka nagyobb f fokánál: pontosan $(\mathrm{gr}(f) + 1)\mathrm{gr}(f)$, mert kompozíció foka a tényezők fokainak szorzata.

3.5.13. Az $f(x, y) = x^9 + x^3y^3 + (y^2 + y)$ már rendezve van x hatványai szerint, a nem nulla együtthatók 1, y^3, $y^2 + y$ relatív prím polinomok $\mathbb{C}[y]$-ban, hiszen az 1 közöttük van: minden normált polinom nyilvánvalóan primitív.

A Schönemann-Eisenstein alkalmazható f-re, mint x polinomjára, a $p = y$ választással. Ez a p prím lesz $\mathbb{C}[y]$-ban, hiszen a $\mathbb{C}[y]$ alaptételes gyűrű, amelyben az y elsőfokú, és így irreducibilis polinom (hiszen $\mathbb{C}$ test). A fenti együtthatók mindegyike y-nal osztható, kivéve a főegyütthatót, vagyis az 1-et, és y^2 nem osztója a konstans tagnak, azaz $y^2 + y$-nak. A Schönemann-Eisenstein tétel minden alaptételes gyűrű fölött ugyanúgy bizonyítható, és így f irreducibilis a $\mathbb{C}[y]$ elemeinek a hányadosaiból álló gyűrű fölött.

Mivel f, mint x polinomja, primitív, a 3.4.6. Tétel általános változata miatt f irreducibilis lesz $\mathbb{C}[y]$ fölött is, azaz $\mathbb{C}[x, y]$-nak ez egy irreducibilis eleme.

3.5.14. Tegyük föl, hogy $\sqrt[3]{4} = a + b\sqrt[3]{2}$, és legyen f az $x^3 - 2$ és az $x^2 - ax - b$ polinomok kitüntetett közös osztója. Mivel $x^3 - 2$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és $f \mid x^3 - 2$, ezért f vagy konstans, vagy $x^3 - 2$ konstansszorosa. Ez utóbbi lehetetlen, mert f osztója a másodfokú $x^2 - ax - b$ polinomnak, és így foka legfeljebb kettő. Tehát f nem nulla konstans polinom.

Az f polinom $\mathbb{C}$ fölött is kitüntetett közös osztó (3.2.3. Gyakorlat). Az $x^3 - 2$ és az $x^2 - ax - b$ polinomoknak $\sqrt[3]{2}$ közös gyöke, és ezért ez gyöke f-nek is (3.2.6. Állítás). Ez lehetetlen, mert f konstans polinom.

3.6. A derivált és a többszörös gyökök.

3.6.1. A deriváltja $6x^5 + 5x^4 + 20x^2 + 12x^2 + 16x + 4$, ennek és az eredeti polinomnak a kitüntetett közös osztója az euklideszi algoritmussal kiszámolva $x^2 + 2$. Tehát f-nek két többszörös gyöke van, ezek $x^2 + 2$ gyökei, vagyis $\pm\sqrt{2}i$, mindegyik kétszeres.

3.6.2. A $3x^2$ jelentése $x^2 + x^2 + x^2$. Ezt a polinomok közötti műveletek definíciója szerint úgy kell kiszámítani, hogy az x^2 együtthatóját (amit nem írtunk ki, mert az értéke 1), önmagával kell háromszor összeadni. Ez az együttható a $\mathbb{Z}_2$ gyűrű eleme, amelyben $1 +_2 1 +_2 1 = 1$. Ezért $3x^2 = 1x^2 = x^2$. Szó sincs tehát arról, hogy $3x^2$ azért lenne x-szel egyenlő, mert mindegyik $x \in \mathbb{Z}_2$-re ugyanazt az értéket veszi föl.

A második gondolatmenetben az a hiba, hogy összekeveredik a polinom és a polinomfüggvény fogalma. Az idézőjeles gondolatmenet csak azt bizonyítja, hogy az x^2 és x polinomokhoz tartozó *polinomfüggvények* egyenlőek. A $\mathbb{Z}_2[x]$ polinomgyűrűben az x határozatlannal formálisan, az együtthatóival modulo 2 kell számolni.

> Ez a példa azt is mutatja, hogy $\mathbb{Z}_2$ fölött nincs értelme polinomfüggvény deriváltjáról beszélni. Hiszen mi is lenne az identikus leképezésnek, mint polinomfüggvénynek a deriváltja? Ezt a polinomfüggvényt az x és az x^2 polinom is megvalósítja. Ezeknek a deriváltja 1, illetve $2x = 0$, és az ezekhez tartozó polinomfüggvények különbözők. Szóval akkor az identitás deriváltja konstans 1, vagy konstans 0 legyen?

3.6.3. Ilyen például $x^9 + x^8$ a $\mathbb{Z}_2$ fölött. A 3.6.3. Állítás bizonyításából látszik, hogy általában olyan $f(x) = (x - b)^8 q(x)$ polinomot érdemes keresni, amelyre $8q(b) = 0$ (de $q(b)$ és $q'(b)$ nem nulla).

3.6.4. Tegyük fel, hogy b az f-nek pontosan ℓ-szeres gyöke, ahol tehát $\ell \geq 1$. Ekkor (a 3.6.4. Tétel szerint) f'-nek a b pontosan $\ell - 1$-szeres gyöke. Tehát $\ell - 1 = k - 1$, vagyis $\ell = k$. Ez a tétel tehát „önmagában hordja a megfordítását".

Az állítás $\mathbb{Z}_2$ fölött nem igaz: az $x^3 + x^2$ polinomnak csak kétszeres gyöke a nulla, annak ellenére, hogy ez a polinom deriváltjának is kétszeres gyöke.

3.6.5. A 3.6.4. Tétel ismételt alkalmazásával világos, hogy ha b az f-nek legalább k-szoros gyöke, akkor a $k-1$-edik deriváltjának legalább egyszeres gyöke, és így közös gyöke f-nek és a $k-1$-edik deriváltjának.

Az állítás megfordítása még $\mathbb{C}$ fölött sem igaz. Például az x^3+x polinomnak az x csak egyszeres gyöke, de a második deriváltnak szintén gyöke.

Ha azt tesszük fel, hogy b gyöke az f első $k-1$ deriváltjának, és $\mathbb{C}$ fölött vagyunk, akkor az előző gyakorlat állításának az ismételt alkalmazásával adódik, hogy f-nek b legalább k-szoros gyöke. Ugyanez $\mathbb{Z}_2$ fölött nem igaz: ismét x^3+x^2 lesz ellenpélda $k=3$ esetén.

3.6.6. Ha egy b komplex szám az f-nek k-szoros gyöke, akkor f'-nek $k-1$-szeres gyöke. Vagyis az $x-b$ irreducibilis polinom kitevője az f kanonikus alakjában k, az f'-ében $k-1$. A kitüntetett közös osztó képlete szerint tehát $x-b$ kitevője (f, f')-ben is $k-1$, azaz b az (f, f')-nek is pontosan $k-1$-szeres gyöke. Így $f_1 = f/(f, f')$-ben az $(x-b)$ irreducibilis tényező kitevője $k-(k-1)=1$ lesz. Más szóval f_1 gyökei ugyanazok, mint az f gyökei, de mindegyik egyszeres, és persze f_1 is racionális együtthatós (a 3.2.3. Gyakorlat miatt).

Ezt a gondolatot alkalmazhatjuk f helyett az (f, f') polinomra is. Mivel ennek gyökei éppen az f legalább kétszeres gyökei, ezért egy szintén racionális együtthatós f_2 polinomot kapunk, amelynek gyökei az f legalább kétszeres gyökei, de mindegyik csak egyszer. Nyilván $g_1(x) = f_1(x)/f_2(x)$ egy olyan racionális együtthatós polinom, amelynek gyökei az f egyszeres gyökei, mindegyik egyszer.

Ezután az állítást k szerinti indukcióval bizonyíthatjuk, a $k=1$ esetet most láttuk be. Ha $k-1$-re már tudjuk az állítást, akkor alkalmazzuk ezt az (f, f') polinomra. Így egy olyan $h(x) \in \mathbb{Q}[x]$ polinomot kapunk, amelynek gyökei pont az (f, f') polinom $k-1$-szeres gyökei, mindegyik egyszer. De akkor h a keresett g_k polinom, hiszen egy komplex szám akkor és csak akkor k-szoros gyöke f-nek, ha $k-1$-szeres gyöke (f, f')-nek.

3.6.7. Ha $f = g^2h$, akkor a szorzat deriválási szabálya szerint $(g^2)' = 2gg'$, és így

$$f' = (g^2)'h + g^2h' = g(2g'h + gh') .$$

Ezért g közös osztója f-nek és f'-nek.

Az x^n-1 deriváltja nx^{n-1}. Ha p nem osztója n-nek, akkor ez nem a nullapolinom $\mathbb{Z}_p[x]$-ben, és így minden osztója sx^k alakú, ahol $0 \neq s \in \mathbb{Z}_p$ (lásd 3.5.1. Gyakorlat). De sx^k csak akkor lehet osztója x^n-1-nek, ha konstans (azaz ha $k=0$), mert x^n-1-nek nem gyöke a 0. Ezért ($p \nmid n$ esetén) x^n-1 relatív prím a deriváltjához, és így nem lehet többszörös tényezője.

Ha viszont $p \mid n$, mondjuk $n = pm$, akkor $\mathbb{Z}_p[x]$-ben

$$x^n - 1 = (x^m - 1)^p .$$

Ez közvetlenül adódik abból, hogy $\mathbb{Z}_p[x]$-ben tagonként lehet p-edik hatványra emelni (3.3.8. Feladat). Ugyanis ekkor $(x^m-1)^p = x^n + (-1)^p$, és $p > 2$ esetén $(-1)^p = -1$, mert p páratlan, ha meg $p=2$, akkor $(-1)^2 = 1$, de ez -1 is, mert $\mathbb{Z}_2$-ben $-1 = 1$. Vagyis x^n-1-nek pontosan $p \mid n$ esetén van többszörös tényezője.

3.6.8. Legyen $f \in S[x]$ egy S fölött irreducibilis polinom, ahol S test, és legyen $h \in S[x]$ az f és f' kitüntetett közös osztója. Tegyük fel, hogy f-nek van többszörös gyöke egy S-nél bővebb T testben. Ekkor (f, f') ebben a nagyobb testben kiszámítva nem konstans. A 3.2.3. Gyakorlat szerint azonban f és f' kitüntetett közös osztója nem függ attól, hogy melyik testben számítjuk ki. Tehát h nem konstans, és mivel osztója az irreducibilis f polinomnak, h és f asszociáltak $S[x]$-ben. Ugyanakkor $h \mid f'$, vagyis beláttuk, hogy $f \mid f'$. Ha $f' \neq 0$, akkor f' foka kisebb f foknál, és így f nem oszthatja f'-t. Tehát csak az $f' = 0$ eset az, ami egyáltalán előfordulhat.

Ha $S = \mathbb{Q}$, akkor ez lehetetlen, hiszen ekkor f konstans polinom lenne, márpedig f-ről föltettük, hogy nem konstans (hiszen irreducibilis).

Ha $S = \mathbb{Z}_2$, és $f(x) = a_0 + \cdots + a_n x^n$, akkor

$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1} = 0$$

akkor és csak akkor teljesül, hogy f páratlan indexű együtthatói nullával egyenlők, vagyis

$$f(x) = a_0 + a_2 x^2 + \cdots + a_{2k} x^{2k}$$

alakú. Vegyük észre, hogy $a_i^2 = a_i$ (hiszen $a_i \in \mathbb{Z}_2$). Mivel $\mathbb{Z}_2$ fölött tagonként lehet négyzetre emelni (3.3.8. Feladat),

$$f(x) = (a_0 + a_2 x + \cdots + a_{2k} x^k)^2 .$$

Ez ellentmond annak, hogy f irreducibilis. Tehát ilyen f polinom $\mathbb{Z}_2$ fölött sincs. Megjegyezzük, hogy ugyanez a gondolatmenet $\mathbb{Z}_2$ helyett szó szerint ugyanígy $\mathbb{Z}_p[x]$-ben is elmondható.

3.6.9. Érdemes általában meggondolni (például n szerinti indukcióval), hogy

$$(f_1 f_2 \dots f_n)' = \sum_{i=1}^{n} f_1 \dots f_{i-1} f_i' f_{i+1} \dots f_n .$$

Ennek az állítás speciális esete, amikor $f_i(x) = x - b_i$ (pontosabban még minden meg van szorozva c-vel). A második állítás az elsőből a b_i behelyettesítésével adódik, hiszen csak egyetlen tagja lesz az összegnek, ami nem (feltétlenül) válik nullává.

3.6.10. Mivel f legalább másodfokú, f' legalább elsőfokú, és így az algebra alaptétele miatt van egy komplex b gyöke. Ekkor $c = -f(b)$ megfelelő lesz. Ehhez a 3.6.5. Következmény miatt elég megmutatni, hogy b közös gyöke $f(x) - f(b)$-nek és a deriváltjának. Ez azonban nyilvánvaló, hiszen ez a derivált $f'(x)$.

3.6.11. Az $f(x)$ a c értéket akkor és csak akkor veszi fel n-nél kevesebb helyen, ha az $f(x) - c$ polinomnak n-nél kevesebb komplex gyöke van, azaz ha van többszörös gyöke. Ez azt jelenti, hogy van egy közös b gyöke a deriváltjával, ami $f'(x)$. Tehát $f'(b) = 0$, és $f(b) = c$. Tehát a kivételes c értékek száma legfeljebb annyi, mint f' komplex gyökeinek a száma, ami legfeljebb $n - 1$, hiszen f' egy $n - 1$-edfokú polinom.

3.7. A rezultáns és a diszkrimináns.

3.7.1. A determinánst például az utolsó sora szerint kifejtve

$$R(f,\,f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = (-2a)(-2ac) + b(ab - 2ab) = 4a^2c - ab^2\,.$$

A diszkrimináns a 3.7.6. Definíció szerint ennek $(-1)^1/a$-szorosa, azaz tényleg $b^2 - 4ac$. A 3.7.8. Állítás szerint ez akkor és csak akkor pozitív, ha minden gyök egyszeres, és a nem valós gyökök száma néggyel osztható. Mivel maximum két gyök van, ez a szám csak úgy lehet néggyel osztható, ha nulla, vagyis mindkét gyök valós. A diszkrimináns akkor és csak akkor nulla, ha a polinomnak egyetlen, kétszeres gyöke van. Ez természetesen csak valós szám lehet, hiszen különben a konjugáltja egy újabb gyöke lenne a polinomnak.

3.7.2. A diszkrimináns (a sok nulla miatt a determinánst ismételt kifejtéssel kiszámolva)

$$(-1)^3 R(f,\,f') = -\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix} = -4p^3 - 27q^2\,.$$

Ennek a diszkussziója a 3.8.2. Tételben található.

3.7.3. Az első egyenletrendszerben a két egyenletet y polinomjának tekintve a rezultánsuk

$$r(x) = \begin{vmatrix} x-1 & x+1 & -2 & 0 \\ 0 & x-1 & x+1 & -2 \\ x-1 & x & -1 & 0 \\ 0 & x-1 & x & -1 \end{vmatrix} = 2(x-1)^2\,.$$

Tudjuk, hogy ha $(x_1,\,y_1)$ közös gyöke az eredeti két egyenletnek, akkor x_1 gyöke a rezultánsnak. A rezultánsnak csak az $x = 1$ gyöke. Azonban ez nem biztos, hogy közös gyökből származik, hiszen a rezultáns akkor is nulla, ha $a_n = b_m = 0$ (és jelenleg ez teljesül, hiszen $a_n = b_m = x - 1$). Tehát az $x = 1$ értéket „kézzel" kell megvizsgálni. Ha $x = 1$, akkor az első egyenlet a $2y - 2 = 0$, a második az $y - 1 = 0$ alakot ölti. Ezeknek $y = 1$ közös gyöke, és így az egyenletrendszer egyetlen megoldása $(x,\,y) = (1,\,1)$.

A második egyenletrendszer esetében a rezultáns $1 - x$ lesz. Az érvelés most is ugyanaz, de most az $x = 1$ hamis gyök, mert ezt visszahelyettesítve a $2y = 1$ és $y = 1$ egyenleteket kapjuk, és ezeknek nincs közös gyöke. A második egyenletrendszernek tehát nincs megoldása.

A harmadik egyenletrendszerben először x-et tekintjük változónak. Az első két egyenlet rezultánsa $f(y,z) = y^4 - (2z+2)y^2 - y + (z^2+z)$. Szimmetriaokokból az első és a

harmadik egyenlet rezultánsa (y és z cseréjével) $g(y,z) = y^2+(-2z^2+1)y+(z^4-2z^2-z)$. Az f és g rezultánsa, rögtön szorzattá alakítva

$$z^5(z+1)^4(z-1)^2(z-2)(z^2+2z+2)(z^2-2z-1)\,.$$

Azt gondolhatnánk, hogy ennek mindegyik gyöke megoldáshoz vezet, hiszen végig normált polinomok rezultánsát vettük, a főegyütthatóknak nem volt gyöke, és így nem jöhetett be „hamis" gyök. De ez tévedés! Például a $z = 2$ gyöke a fenti polinomnak. Ez annyit jelent, hogy az $f(y,2)$ és a $g(y,2)$ polinomoknak van közös gyöke. Valóban van: az $y = 1$ (és csak ez). Tehát ha $y = 1$ és $z = 2$, akkor az egyenletrendszer első két egyenletének is kell legyen közös gyöke x-re. Van is: az $x = -2$ (és más nem). Ugyanígy a második két egyenletnek is kell legyen közös gyöke, ez viszont csak az $x = -2$ lesz. Ez az oka annak, hogy a $z = 2$ végülis nem vezet az egyenletrendszer megoldásához.

Az összes gyököt ugyanígy végigszámolni nagyon fáradságos volna. Egyszerűbb megoldáshoz vezet, ha az f polinom helyett az egyenletrendszer második és harmadik egyenletének a rezultánsát számoljuk ki, ez $h(x,y) = y^2 + y - (z^2 + z)$. A g és a h rezultánsa ugyanis

$$z^4(z+1)^2(z^2-2z-1)$$

(ezt szorzattá alakítani is sokkal egyszerűbb, mint a fenti polinomot, hiszen csak a racionális gyöktesztre van ehhez szükség). A fentiek szerint ennek is valamennyi gyökét ellenőrizni kell. A végeredmény a következő: a megoldások egyrészt azok, ahol két ismeretlen értéke nulla, a harmadik pedig -1, másrészt azok, ahol $x = y = z$ a $z^2 - 2z - 1$ egyenlet valamelyik gyökével (azaz $1 \pm \sqrt{2}$-vel) egyenlő.

3.8. A harmad- és negyedfokú egyenlet.

3.8.1. Tegyük föl először, hogy $b^2 - 4ac = 0$. Ha $a \neq 0$, akkor $b^2 - 4ac$ a polinom diszkriminánsa. Mivel ez nulla, van kétszeres gyök, így a polinom $a(x-\alpha)^2$ alakú. Itt persze az $a \in \mathbb{C}$ számból is vonható négyzetgyök. Ha viszont $a = 0$, akkor $b^2 = 4ac$ miatt $b = 0$, vagyis a polinom konstans, és így ismét teljes négyzet.

Megfordítva, ha a polinom teljes négyzet, akkor vagy egy konstans polinom négyzete, vagy egy elsőfokúé. Az első esetben konstans polinomról van szó, tehát $b^2 = 4ac = 0$. A második esetben a polinom másodfokú, és mivel egy elsőfokú polinom négyzete, van kétszeres gyöke. Ezért a diszkriminánsa nulla kell, hogy legyen.

3.8.2.

(1) $x^3 - 6ix - i + 8 = 0$: a diszkrimináns szerencsére teljes négyzetté alakítható: $D = (8-i/2)^2 - (2i)^3 = (8+i/2)^2$. Innen $u = \cos 30^\circ + i \sin 30^\circ$ és $v = 2i/u = 2(\cos 60^\circ + i \sin 60^\circ)$, a gyökök $(1+\sqrt{3}/2)+(1/2+\sqrt{3})i$, $(1-\sqrt{3}/2)+(1/2-\sqrt{3})i$ és $-2-i$.

(2) $x^3 + 12x - 16i = 0$: itt a diszkrimináns nulla, innen $u = 2(\cos 30^\circ + i \sin 30^\circ)$, $v = -4/u = 2(\cos 150^\circ + i \sin 150^\circ)$, $x^3 + 12x - 16i = (x-2i)^2(x+4i)$, azaz a $2i$ kétszeres gyök.

(3) $x^3 - 21x + 20 = 0$: ennél az egyenletnél $D = -243$, és így nemtriviális feladat a köbgyökvonás. Trigonometrikus alakban közelítőleg elvégezhetjük (kalkulátorral végezve a trigonometrikus alakra való oda- és visszakonvertálást), ekkor $u = \sqrt{7}(\cos\alpha + i\sin\alpha)$ adódik, ahol $\alpha \approx 40.893^\circ$. Az 1.2. Szakaszban ezt az egyenletet megoldottuk: u értéke valójában $2 + i\sqrt{3}$, a gyökök 4, 1 és -5.

(4) $x^4 + x^2 + 4x - 3 = 0$: a harmadfokú rezolvens $8u^3 - 4u^2 + 24u - 28$, aminek szerencsére gyöke az 1. Ennek alapján az egyenlet két másodfokú polinom szorzataként $(x^2 + 1)^2 - (x - 2)^2 = (x^2 - x + 3)(x^2 + x - 1)$ alakban írható, gyökei tehát $(1 \pm i\sqrt{11})/2$ és $(-1 \pm \sqrt{5})/2$.

3.8.3. A harmadfokú rezolvens $(8u - 40)(u^2 - 1)$, ennek gyökei $u = 1$, $u = -1$, $u = 5$. Ezekből rendre az $x^4 - 10x^2 + 1$ polinom következő felbontásait kapjuk:

$$(x^2 + 1)^2 - 12x^2 = (x^2 - 2\sqrt{3}x + 1)(x^2 + 2\sqrt{3}x + 1)$$
$$(x^2 - 1)^2 - 8x^2 = (x^2 - 2\sqrt{2}x - 1)(x^2 + 2\sqrt{2}x - 1)$$
$$(x^2 - 5)^2 - 24 = (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6})\,.$$

Ezek pontosan a 3.3.10. Feladatban használt felbontások.

Egy negyedfokú polinomnak négy gyöke van, ezek háromféleképpen állíthatók párba, és így háromféle felbontása van két másodfokú szorzatára. Általában is megmutatható, hogy ezek pont a harmadfokú rezolvens három gyökéből kaphatók, a negyedfokú egyenlet megoldásában leírt módszerrel.

3.8.4. Feltehetjük, hogy az eredeti polinom normált. Ha van racionális gyöke, akkor egy első és egy harmadfokú szorzatára bontható. Ha a harmadfokú rezolvensnek van racionális gyöke, akkor az eredeti polinomot ennek segítségével két másodfokú szorzatára bontva nyilván racionális együtthatós tényezők keletkeznek. Ilyenkor tehát a polinom reducibilis $\mathbb{Q}$ fölött.

Megfordítva, tegyük fel, hogy egy negyedfokú, normált $f \in \mathbb{Q}[x]$ polinom reducibilis a racionális számtest fölött. Ekkor vagy egy első és egy harmadfokú, vagy két másodfokú polinom szorzatára bontható. Az első esetben van racionális gyöke. A második esetben nyilván feltehető, hogy $f(x) = (x^2 + vx + w)(x^2 + sx + t)$, ahol $v, w, s, t \in \mathbb{Q}$. Meg szeretnénk mutatni, hogy ez a felbontás a harmadfokú rezolvens felhasználásával is megkapható, azaz hogy ebben az esetben a harmadfokú rezolvensnek van racionális gyöke.

Az $f(x) = x^4 + ax^3 + bx^2 + cx + d = (x^2 + vx + w)(x^2 + sx + t)$ egyenlőségből beszorzás után leolvashatók az a, b, c, d együtthatóknak a v, w, s, t-vel kifejezett értékei. Ezután a harmadfokú rezolvens képletébe az $u = (w + t)/2$ kifejezést behelyettesítve v, w, s, t-ben azonosságot kapunk, tehát a racionális $(w + t)/2$ szám tényleg gyöke a harmadfokú rezolvensnek. A részletek kiszámítását az olvasóra hagyjuk.

A most elhangzott megoldás nagyon számolós, és az sem világos belőle, hogyan jut az ember eszébe pont az $u = (w + t)/2$ értékkel próbálkozni. Az alábbi gondolatmenet e két szempontból jobb, bár kicsit talán bonyolultabb.

A negyedfokú egyenlet megoldásakor látott módszerben $f = K^2 - L^2 = (K-L)(K+L)$, ahol K másodfokú, L elsőfokú. Ha ebből a fenti felbontást akarjuk megkapni, akkor azt szeretnénk, hogy $K(x) + L(x) = x^2 + vx + w$ és $K(x) - L(x) = x^2 + sx + t$ teljesüljön. A két egyenletet összeadva, és kettővel elosztva $K(x) = x^2 + (v+s)x/2 + (w+t)/2$ adódik. Másrészt a negyedfokú egyenlet megoldásakor $K(x) = x^2 + ax/2 + u$ volt, ahol u a harmadfokú rezolvens gyöke. *Ezért* kézenfekvő azt kipróbálni, hogy $u = (w+t)/2$ tényleg gyöke-e a harmadfokú rezolvensnek.

Valójában ezt a behelyettesítést sem kell elvégezni. Ha ugyanis a fenti két egyenlet kivonásával L-et is kiszámoljuk, akkor $L(x) = (v-s)x/2 + (w-t)/2$ adódik. Beszorzással nyilvánvaló, hogy f-ben az x^3-ös tag együtthatója $a = v+s$. Így az alábbi azonosság teljesül:

$$f(x) = \Big(x^2 + \frac{a}{2}x + \frac{w+t}{2}\Big)^2 - \Big(\frac{v-s}{2}x + \frac{w-t}{2}\Big)^2.$$

Ha $u = (w+t)/2$, akkor tehát K ugyanaz, mint a negyedfokú egyenlet megoldásában szereplő átalakításban. Ezért a polinom fennmaradó, másodfokú része is ugyanaz. Képletben:

$$\Big(\frac{v-s}{2}x + \frac{w-t}{2}\Big)^2 = \Big(2u + \frac{a^2}{4} - b\Big)x^2 + \Big(au - c\Big)x + \Big(u^2 - d\Big).$$

Tehát ez a polinom erre az u értékre teljes négyzet, és ezért a diszkriminánsa nulla (3.8.1. Gyakorlat). Ez a diszkrimináns pont az egyenlet harmadfokú rezolvense, és így ennek gyöke az $u = (w+t)/2$.

3.8.5. A 3.5.8. Feladat szerint minden n-edfokú $f(x) = a_n x^n + \cdots + a_0$ reciprok polinom szimmetrikus a „közepére", vagyis $a_n = a_0$, $a_{n-1} = a_1$, és így tovább, általában $a_i = a_{n-i}$. Ha f foka páratlan, akkor i és $n-i$ közül egy páros, egy páratlan, és így $a_i x^i + a_{n-i}x^{n-i}$-nek gyöke a -1. A polinom ilyen tagok összege, tehát annak is gyöke a -1.

A feladatban szereplő $x^7 + 2x^6 - x^4 - x^3 + 2x + 1$ polinomból az $x+1$ gyöktényezőt kiemelve $x^6 + x^5 - x^4 - x^2 + x + 1$ marad. Ennek nem gyöke a nulla, és így gyökvesztés nélkül eloszthatjuk x^3-nel, vagyis egyenletünk a következőképpen alakul:

$$0 = \frac{x^6 + x^5 - x^4 - x^2 + x + 1}{x^3} = \Big(x^3 + \frac{1}{x^3}\Big) + \Big(x^2 + \frac{1}{x^2}\Big) - \Big(x + \frac{1}{x}\Big).$$

Legyen $z = x + (1/x)$, ekkor négyzetre illetve köbre emeléssel

$$z^2 = \Big(x^2 + \frac{1}{x^2}\Big) + 2 \quad \text{és} \quad z^3 = \Big(x^3 + \frac{1}{x^3}\Big) + 3\Big(x + \frac{1}{x}\Big).$$

Ezért egyenletünk a $z^3 - 3z + z^2 - 2 - z = 0$ alakot ölti. Ez harmadfokú, tehát meg tudjuk oldani gyökjelekkel. Innen az eredeti polinom gyökeit is megkapjuk, mert ha $z = u$ a fenti harmadfokú egyenlet valamelyik gyöke (ahol u már ismert szám), akkor az $x + (1/x) = u$ egyenletet x-szel átszorozva másodfokú egyenletet kapunk.

Általában is könnyen belátható, hogy egy páros fokú reciprok polinom mindig felírható a $z = x + (1/x)$ polinomjaként. Ezért a gyökeinek a meghatározása visszavezethető egy feleakkora fokú egyenlet megoldására.

3.8.6. Ezt az egyenletet, a negyedfokú egyenlet megoldási ötletéhez hasonlóan, két négyzet különbségére bonthatjuk. Mivel $-2x^2-4x-2=-2(x+1)^2=(i\sqrt{2})^2(x+1)$, ezért

$$x^8+2x^2+4x+2=(x^4)^2-(i\sqrt{2}x+i\sqrt{2})^2=$$
$$=(x^4-i\sqrt{2}x-i\sqrt{2})(x^4+i\sqrt{2}x+i\sqrt{2})\,.$$

Tehát csak két negyedfokú egyenletet kell megoldani.

3.9. A körosztási polinom.

3.9.1. A harmadik primitív egységgyökök $-1/2\pm i\sqrt{3}/2$, a hatodikak $1/2\pm i\sqrt{3}/2$, a tizenkettedikek $\pm\sqrt{3}/2\pm i/2$. Innen az állítás beszorzással adódik.

3.9.2. A p darab p-edik egységgyök az x^p-1 polinom összes gyöke (és mindegyik egyszeres, lásd 2.5.10. Feladat). A 1.5.8. Tétel szerint ezek közül az 1 kivételével mindegyik primitív p-edik egységgyök is, hiszen az $1,\dots,p-1$ számok relatív prímek p-hez. Ezért

$$\Phi_p(x)=\frac{x^p-1}{x-1}=1+x+\dots+x^{p-1}\,.$$

3.9.3. Ha $o(\eta)=12$, akkor hatványai között négy tizenkettedrendű, két hatodrendű, két negyedrendű, két harmadrendű, egy másodrendű és egy elsőrendű szám van. Az adódik, hogy $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)=x^{12}-1$. Az osztás elvégzésekor érdemes a nevezőben minél több tényezőt összevonni, mert ezzel a számolást rövidíthetjük. A 6 osztóihoz tartozó körosztási polinomok szorzata x^6-1, ezért

$$\Phi_{12}(x)=\frac{x^{12}-1}{\Phi_1\Phi_2\Phi_3\Phi_6\Phi_4}=\frac{x^{12}-1}{(x^6-1)\Phi_4(x)}=\frac{x^6+1}{x^2+1}=x^4-x^2+1\,.$$

3.9.4. Tekintsük a $\prod_{d|n}\Phi_d(x)=x^n-1$ képletben a fokszámokat.

3.9.5. A rekurziós képlet alapján, ha p prím, akkor

$$\Phi_{p^k}(x)=\frac{x^{p^k}-1}{\Phi_1\Phi_p\dots\Phi_{p^{k-1}}}=\frac{x^{p^k}-1}{x^{p^{k-1}}-1}\,,$$

hiszen a nevezőben szereplő indexek éppen p^{k-1} osztói. Az $y=x^{p^{k-1}}$ helyettesítéssel azonnal látszik, hogy mennyi ennek a törtnek az értéke:

$$\Phi_{p^k}(x)=\frac{y^p-1}{y-1}=1+y+\dots+y^{p-1}=1+x^{p^{k-1}}+x^{2p^{k-1}}+\dots+x^{(p-1)p^{k-1}}\,.$$

3.9.6. Legyen n pozitív, páratlan egész. A 1.5.10. Feladat szerint ha $o(\varepsilon) = n$, akkor $o(-\varepsilon) = 2n$, és ha $o(\varepsilon) = 2n$, akkor $o(-\varepsilon) = n$. Ez azt jelenti, hogy $\varepsilon \mapsto -\varepsilon$ kölcsönösen egyértelmű megfeleltetést létesít Φ_n és Φ_{2n} gyökei között. Más szóval $\Phi_n(-x)$ és $\Phi_{2n}(x)$ gyökei ugyanazok (és mindegyik egyszeres). Ezért e két polinom egymás konstansszorosa. A Φ_{2n} polinom normált, tehát a két polinom egyenlőségéhez már csak azt kell megmutatni, hogy (páratlan $n > 1$ esetén) $\Phi_n(-x)$ is az. De ez igaz: a $\Phi_n(-x)$ főegyütthatója $(-1)^{\varphi(n)} = 1$, mert a B.0.7. Állítás szerint $\varphi(n)$ páros szám (kivéve ha $n = 1$ vagy 2).

3.9.7. Láttuk, hogy $\Phi_1(x) = x - 1$. Ha p prímszám, akkor a 3.9.2. Gyakorlat miatt $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$. A további prímhatvány-indexű körosztási polinomok 20-ig a 3.9.5. Gyakorlat alapján a következők: $\Phi_4(x) = x^2+1$, $\Phi_8(x) = x^4+1$, $\Phi_{16}(x) = x^8+1$, $\Phi_9(x) = x^6+x^3+1$. Ha az index egy páratlan szám kétszerese, akkor az előző feladat miatt $\Phi_6(x) = x^2-x+1$, $\Phi_{10}(x) = x^4-x^3+x^2-x+1$, $\Phi_{14}(x) = x^6-x^5+x^4-x^3+x^2-x+1$, $\Phi_{18}(x) = x^6 - x^3 + 1$. Korábban kiszámoltuk már azt is, hogy $\Phi_{12}(x) = x^4 - x^2 + 1$. A megmaradt esetek: $\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ (ezt a rekurziós képletből osztással kaphatjuk), és $\Phi_{20}(x) = \Phi_{10}(x^2)$ (lásd a 3.9.9. Feladatot).

3.9.8. Tudjuk, hogy $x^{n/d} - 1$ azoknak az $x - \eta$ gyöktényezőknek a szorzata, ahol η rendje osztója n/d-nek. Azt kell belátnunk, hogy a $\prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$ képletben $o(\eta) = n$ esetén $x - \eta$ az első hatványon szerepel, egyébként pedig a nulladikon. Legyen $o(\eta) = m$. Ekkor $x^{n/d} - 1$-ben $x - \eta$ az első hatványon szerepel, ha $m \mid (n/d)$, egyébként pedig a nulladikon. Persze $m \mid (n/d) \iff d \mid (n/m)$. Ezért a $\prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$ képletben $x - \eta$ kitevője $\sum_{d|(n/m)} \mu(d)$. A B.0.10. Állítás miatt ez az összeg 1, ha $n/m = 1$, és nulla egyébként.

3.9.9. A feladatra két megoldást adunk. Az első rövid számolás, ami felhasználja a 3.9.8. Feladatban bizonyított összefüggést. A második bizonyítás hosszabb, de nagyon tanulságos, mert gyakoroljuk általa az elemrend fogalmát.

Az első bizonyításban tehát induljunk ki abból, hogy $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$. Ebben a szorzatban eltekinthetünk azoktól a tényezőktől, amelyekre a $\mu(d)$ kitevő nulla, hiszen az ilyen tényezők értéke 1. Tehát csak azok a $d \mid n$ számok az érdekesek, amelyek csupa különböző prímek szorzatai. Mivel n minden prímosztója osztója m-nek is, az ilyen d számok m-nek is osztói. Ezért

$$\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)} = \prod_{d|m}\left((x^{n/m})^{m/d} - 1\right)^{\mu(d)} = \Phi_m(x^{n/m})$$

(az utolsó lépésben m-re alkalmaztuk a 3.9.8. Feladatban bizonyított formulát).

A második, közvetlen bizonyításban a

$$\Phi_n(x) = \prod_{o(\eta)=n}(x - \eta) \quad \text{és} \quad \Phi_m(x^{n/m}) = \prod_{o(\varepsilon)=m}(x^{n/m} - \varepsilon)$$

képletekből indulunk ki. Mindkét képletben könnyen láthatóan minden gyök egyszeres, tehát azt kell megmutatni, hogy a két oldalnak ugyanazok a gyökei. Más szóval, hogy $o(\eta) = n$ akkor és csak akkor, ha $o(\eta^{n/m}) = m$.

A hatvány rendjének képlete szerint $o(\eta^{n/m}) = o(\eta)/(o(\eta), n/m)$. Ha $o(\eta) = n$, akkor ez $n/(n, n/m) = n/(n/m) = m$. Megfordítva, tegyük fel, hogy $o(\eta)/(o(\eta), n/m) = m$. Azaz

$$o(\eta) = (o(\eta), n/m)m = (o(\eta)m, n) = (m, n/o(\eta))o(\eta)\,.$$

Itt kétszer használtuk a kitüntetett közös osztó kiemelési tulajdonságát. (A második esetben is szabad ezt megtenni, azaz $o(\eta) \mid n$, hiszen ez már az $o(\eta) = (o(\eta)m, n)$ összefüggésből következik.) Azt kaptuk tehát, hogy $(m, n/o(\eta)) = 1$. Ha az $n/o(\eta)$ számnak lenne egy p prímosztója, akkor persze $p \mid n$, és a feltételünk szerint n prímosztói mind osztják m-et, azaz $p \mid m$, ahonnan a $p \mid (m, n/o(\eta)) = 1$ ellentmondás adódik. Ezért az $n/o(\eta)$ egész számnak nincs prímosztója, vagyis $n/o(\eta) = 1$, ami a kívánt $o(\eta) = n$ állítást bizonyítja.

3.9.10. Az előző feladat alapján elég a négyzetmentes indexű körosztási polinomokat ismerni. Ha ugyanis az n szám tetszőleges, és az m az n prímosztóinak a szorzata, akkor m négyzetmentes, és Φ_m ismeretében $\Phi_n(x) = \Phi_m(x^{n/m})$ is kiszámítható. Speciálisan $\Phi_{36}(x) = \Phi_6(x^6) = x^{12} - x^6 + 1$, $\Phi_{72}(x) = \Phi_6(x^{12}) = x^{24} - x^{12} + 1$, $\Phi_{144}(x) = \Phi_6(x^{24}) = x^{48} - x^{24} + 1$, $\Phi_{100}(x) = \Phi_{10}(x^{10}) = x^{40} - x^{30} + x^{20} - x^{10} + 1$ (itt felhasználtuk a 3.9.7. Gyakorlat eredményét).

3.9.11. Belátjuk, hogy az n-edik primitív egységgyökök összege $\mu(n)$, ahol μ a Möbius-függvény (B.0.9. Definíció), szorzatuk pedig mindig 1, kivéve az $n = 2$ esetet, amikor -1. Az utóbbi állítást az olvasónak érdemes bebizonyítania úgy is, hogy minden primitív n-edik egységgyököt párosít az inverzével (ami szintén primitív n-edik egységgyök). Mi mindkét állítást a gyökök és együtthatók összefüggésének felhasználásával igazoljuk. Ezek alapján ugyanis a primitív n-edik egységgyökök $S(n)$ összege a $\Phi_n(x)$ körosztási polinomban a „felülről második tag", vagyis az $x^{\varphi(n)-1}$-es tag együtthatójának ellentettje, szorzatuk pedig a konstans tag $(-1)^{\varphi(n)}$-szerese.

A $\prod_{d|n} \Phi_d(x) = x^n - 1$ összefüggésben nézzük meg, mi az x^{n-1} együtthatója a két oldalon. A jobboldalon ez 0, kivéve az $n = 1$ esetet, amikor -1. A másik oldalon x^{n-1}-es tagot csak úgy kaphatunk, ha egy kivételével mindegyik polinomból a legmagasabb fokú tagot vesszük, a kivételesből pedig a második legmagasabb fokút (hiszen $n - 1$ csak eggyel kevesebb, mint a szorzatpolinom foka). Mivel $\Phi_d(x)$-ben a második legmagasabb fokú tag együtthatója $-S(d)$, és az összes Φ_d polinom normált, a baloldalon az x^{n-1} együtthatója a $-S(d)$ számok összege lesz. A két oldalt egybevetve tehát beláttuk, hogy

$$\sum_{d|n} S(d) = \begin{cases} 1 & \text{ha } n = 1, \\ 0 & \text{ha } n \neq 1. \end{cases}$$

Ez ugyanaz az összefüggés, amit a B.0.10. Állításban igazoltunk S helyett μ-re. Ezért n szerinti indukcióval azonnal látjuk, hogy $S(n) = \mu(n)$. (Valójában arról van szó, hogy ez a rekurzív összefüggés az S függvényt egyértelműen definiálja. Az indukciót most is ugyanazzal a logikával végezzük, mint a 3.9.3. Következmény bizonyításában.)

A szorzatra vonatkozó összefüggést levezetéséhez a $\prod_{d|n}\Phi_d(x) = x^n - 1$ konstans tagját kell tekinteni (azaz nullát helyettesíteni). Ekkor $\prod_{d|n}\Phi_d(0) = -1$ adódik, és innen indukcióval látszik, hogy $\Phi_n(0)$ értéke mindig 1, kivéve $n = 1$-re, amikor -1. Tudjuk, hogy $\varphi(n)$ akkor és csak akkor páros, ha $n > 2$ (lásd B.0.7. Állítás). Az n-edik primitív egységgyökök szorzata, ami $(-1)^{\varphi(n)}\Phi_n(0)$, tehát tényleg 1 ha $n \neq 2$, és -1, ha $n = 2$.

3.9.12. A $\Phi_n(1)$ értéket kell meghatároznunk. A $\prod_{d|n}\Phi_d(x) = x^n - 1$ összefüggésbe közvetlenül 1-et helyettesíteni nem érdemes, hiszen a Φ_1 miatt nullát kapunk. Ezért előbb osszunk le $\Phi_1(x) = x - 1$-gyel. Az eredmény:

$$\prod_{\substack{d|n\\ d\neq 1}}\Phi_d(x) = \frac{x^n-1}{x-1} = 1 + x + x^2 + \cdots + x^{n-1}\,.$$

Ebbe az azonosságba $x = 1$-et helyettesítve

$$\prod_{\substack{d|n\\ d\neq 1}}\Phi_d(1) = n\,.$$

Innen könnyen látható n szerinti indukcióval, hogy ha n egy p prím hatványa, de nem 1, akkor $\Phi_n(1) = p$, ha pedig n nem prímhatvány, akkor $\Phi_n(1) = 1$. Természetesen $n = 1$-re közvetlenül látszik, hogy az eredmény nulla.

Felmerül a kérdés, hogy szabad-e a fenti egyenlőségbe $x = 1$-et helyettesíteni, nem jelentené-e ez azt, hogy $1 - 1 = 0$-val osztottunk. A válasz megtalálható a 2.5.10. Feladat megoldását követő diszkusszióban.

3.9.13. Eljárhatnánk az előző feladat megoldásában használt módon is, $\Phi_2(x) = x+1$-gyel leosztva a rekurziót páros n esetén. Ennél egyszerűbb azonban, ha ennek a feladatnak az *eredményét* használjuk fel. Ha $n = 4m$, akkor a 3.9.9. Feladat miatt $\Phi_n(x) = \Phi_{2m}(x^2)$, és így $\Phi_n(-1) = \Phi_{2m}(1)$, ami 2, ha m kettő-hatvány, különben 1. Ha n nem osztható néggyel, akkor a 3.9.6. Gyakorlat miatt páratlan $n > 1$ esetén az eredmény $\Phi_{2n}(1) = 1$, ha viszont $n = 2k > 2$, akkor $\Phi_n(-1) = \Phi_k(1)$. A fennmaradó „kis" eseteket kézzel kiszámolhatjuk. A végeredmény a következő: $\Phi_1(-1) = -2$, $\Phi_2(-1) = 0$, $\Phi_n(-1) = 2$, ha $n > 2$ kettő-hatvány, $\Phi_n(-1) = p$, ha $n = 2p^k > 2$ (p prím), a többi esetben az eredmény 1.

3.9.14. Legyen θ egy mn-edik primitív egységgyök. Mivel m és n relatív prímek, vannak olyan x és y egészek, melyekre $nx + my = 1$. Ekkor $\theta = \theta^{nx+my} = \theta^{nx}\theta^{my}$. A hatvány rendjének képlete szerint $o(\theta^{nx}) = mn/(mn, nx)$. Nyilván $(mn, nx) = n(m, x)$, és az $nx + my = 1$ összefüggés miatt $(m, x) = 1$. Ezért $o(\theta^{nx}) = m$. Hasonlóan $o(\theta^{my}) = n$. Ezért θ tényleg előáll egy primitív m-edik és egy primitív n-edik egységgyök szorzataként.

Most belátjuk, hogy ez az előállítás egyértelmű. Tegyük fel, hogy $o(\eta) = o(\eta') = m$ és $o(\varepsilon) = o(\varepsilon') = n$. Ha $\eta\varepsilon = \eta'\varepsilon'$, akkor innen $\eta/\eta' = \varepsilon'/\varepsilon$. A baloldalon egy m-edik, a jobboldalon egy n-edik egységgyök van, azaz a baloldal rendje m-nek, a jobboldalé n-nek

osztója. Mivel $(m, n) = 1$, ez csak úgy lehet, hogy az egyenlőség mindkét oldalán 1 rendű szám áll, azaz $\eta = \eta'$ és $\varepsilon = \varepsilon'$.

Az Euler-függvény multiplikativitásának bizonyításához tekintsük az összes $\eta\varepsilon$ szorzatot, ahol $o(\eta) = m$ és $o(\varepsilon) = n$. Az előző bekezdésben bizonyított állítás szerint az ilyen szorzatok száma $\varphi(m)\varphi(n)$. Az 1.5.12. Gyakorlat (3) pontja szerint az így kapott $\eta\varepsilon$ szorzatok mind mn rendű számok, és az első bekezdés szerint minden mn rendű szám előáll egy ilyen szorzatként. Ezért ezek a szorzatok éppen az mn-edik primitív egységgyököket adják, és így számuk $\varphi(mn)$.

3.9.15. Az előző gyakorlat miatt

$$\Phi_{mn}(x) = \prod_{o(\eta)=m,\ o(\varepsilon)=n} (x - \eta\varepsilon) = \left(\prod_{o(\eta)=m} \eta \right)^{\varphi(n)} \prod_{o(\eta)=m,\ o(\varepsilon)=n} (x/\eta - \varepsilon)\,.$$

A zárójelben álló szorzat a 3.9.11. Feladat miatt 1, kivéve az $m = 2$ esetet, amikor -1, ez adja a minusz előjelet az $m = 2$, $n = 1$ esetben. Csoportosítsunk η szerint:

$$\prod_{o(\eta)=m,\ o(\varepsilon)=n} (x/\eta - \varepsilon) = \prod_{o(\eta)=m} \left(\prod_{o(\varepsilon)=n} (x/\eta - \varepsilon) \right) = \prod_{o(\eta)=m} \Phi_n(x/\eta)\,.$$

Tudjuk, hogy ha η befutja az m-edik primitív egységgyököket, akkor $1/\eta$ is, és ezért ha x/η helyett ηx-et írunk, azzal csak a tényezők sorrendjét változtatjuk.

3.9.16. $\mathbb{Z}$ fölött a körosztási polinomok az irreducibilis tényezők:

$$x^{12} - 1 = \Phi_1(x)\ \Phi_2(x)\ \Phi_3(x)\ \Phi_4(x)\ \Phi_6(x)\ \Phi_{12}(x) = (x - 1)(x + 1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)(x^4 - x^2 + 1)\,.$$

A $\mathbb{Z}_2$ fölött ez tovább bomlik a következőképpen:

$$\Phi_4(x) = (x + 1)^2\,, \quad \Phi_{12}(x) = (x^2 + x + 1)^2\,,$$

azaz $x^{12} - 1 = (x + 1)^4(x^2 + x + 1)^4$. A $\mathbb{Z}_3$ fölött

$$\Phi_3(x) = (x - 1)^2\,, \quad \Phi_6(x) = (x + 1)^2\,, \quad \Phi_{12}(x) = (x^2 + 1)^2\,,$$

azaz $x^{12}-1 = (x-1)^3(x+1)^3(x^2+1)^3$ (az x^2+1 irreducibilis $\mathbb{Z}_3$ fölött, hiszen másodfokú, és nincs gyöke $\mathbb{Z}_3$-ban). Végül $\mathbb{Z}_5$ fölött

$$\Phi_4(x) = (x - 2)(x + 2)\,, \quad \Phi_{12}(x) = (x^2 + 2x - 1)(x^2 - 2x - 1)\,.$$

A kapott eredményeket érdemes összevetni a 3.9.17. Feladat állításával.

3.9.17. Tegyük fel, hogy n a legkisebb ellenpélda az állításra. Végig $\mathbb{Z}_p[x]$-ben számolunk (de nem írjuk ki a felülvonásokat). Tekintsük a $\prod_{d|n}\Phi_d(x)=x^n-1$ összefüggést. A d szám egyértelműen felírható $d=p^jm'$ alakban, ahol $0\le j\le k$ és $m'\mid m$. Az indukciós feltevés szerint $d<m$ esetén teljesül $\mathbb{Z}_p$ fölött, hogy $\Phi_d=\Phi_{m'}^{\varphi(p^j)}$. Gyűjtsük össze rögzített m' mellett ezeket a tényezőket. Az eredmény

$$\Phi_{m'}^{\varphi(p^0)+\varphi(p^1)+\cdots+\varphi(p^k)}=\Phi_{m'}^{p^k}$$

(a kitevőben a 3.9.4. Gyakorlatban bizonyított $\sum_{d|p^k}\varphi(d)=p^k$ összefüggést használtuk). Ha a $\Phi_d=\Phi_{m'}^{\varphi(p^j)}$ összefüggést a $d=n$ esetben is tudnánk (ez a bizonyítandó állítás), akkor a fentieket összeszorozva, és felhasználva, hogy $\prod_{m'|m}\Phi_{m'}(x)=x^m-1$,

$$\prod_{d|n}\Phi_d(x)=\left(\prod_{m'|m}\Phi_{m'}(x)\right)^{p^k}=(x^m-1)^{p^k}=x^{mp^k}-1=x^n-1$$

adódna (hiszen mod p szabad tagonként p^k-adik hatványra emelni, és $(-1)^{p^k}=-1$ páratlan p prímre is, meg $p=2$-re is igaz, utóbbi azért, mert $\mathbb{Z}_2$-ben $-1=1$). Ha most úgy számolunk, hogy a $\Phi_n=\Phi_m^{\varphi(p^k)}$ összefüggést nem használjuk, akkor ugyanez a gondolatmenet azt adja, hogy

$$\frac{\Phi_m(x)^{\varphi(p^k)}}{\Phi_n(x)}\prod_{d|n}\Phi_d(x)=x^n-1\,.$$

Felhasználva, hogy $\prod_{d|n}\Phi_d(x)=x^n-1$, azt kapjuk, hogy a baloldali tört értéke 1, vagyis $\Phi_n(x)=\Phi_m(x)^{\varphi(p^k)}$, amit bizonyítani kellett. Valamivel talán egyszerűbb a számolás, ha a fenti módszerrel csak az $n=pm$ esetet intézzük el, majd alkalmazzuk a 3.9.9. Feladatot.

3.9.18. A 3.9.5. Gyakorlat képlete alapján

$$\Phi_{p^k}(x)=\frac{x^{p^k}-1}{x^{p^{k-1}}-1}=1+x^{p^{k-1}}+x^{2p^{k-1}}+\cdots+x^{(p-1)p^{k-1}}\,.$$

Ezért $\Phi_{p^k}(x+1)$ konstans tagja az $x=0$ helyen vett helyettesítési érték, vagyis p. Továbbá $\mathbb{Z}_p[x]$-ben számolva

$$\Phi_{p^k}(x+1)=\frac{(x+1)^{p^k}-1}{(x+1)^{p^{k-1}}-1}=\frac{x^{p^k}+1-1}{x^{p^{k-1}}+1-1}=x^{p^k-p^{k-1}}\,.$$

Ez $\mathbb{Z}$-ben azt jelenti, hogy $\Phi_{p^k}(x+1)$ minden együtthatója osztható p-vel, kivéve a főegyütthatót. A Schönemann-Eisenstein kritérium tehát teljesül.

3.9.19. A 3.9.18. Gyakorlat és a 3.9.6. Feladat alapján látjuk, hogy prímhatványra, illetve páratlan prímhatvány kétszeresére a körosztási polinom egy eltoltja tényleg teljesíti a Schönemann-Eisenstein kritérium feltételét. Megfordítva, tegyük fel, hogy $\Phi_n(x+c)$ a p prímre teljesíti a kritériumot. Áttérve $\mathbb{Z}_p$-re azt kapjuk, hogy $\overline{\Phi_n}(x+\overline{c}) = x^{\varphi(n)}$, hiszen a főegyüttható kivételével minden együttható eltűnik mod p. Ebbe az azonosságba $y = x - \overline{c}$-t írva adódik, hogy $\overline{\Phi_n}(y) = (y-\overline{c})^{\varphi(n)}$.

Legyen $n = p^k m$, ahol már $p \nmid n$. A 3.9.17. Feladat szerint $\overline{\Phi_n}(y) = \overline{\Phi_m}(y)^{\varphi(p^k)}$, és így

$$\overline{\Phi_m}(y) = (y-\overline{c})^{\frac{\varphi(n)}{\varphi(p^k)}} = (y-\overline{c})^{\varphi(m)}\,.$$

Tudjuk, hogy $\Phi_m(y) \mid y^m - 1$. Mivel $p \nmid m$, az $y^m - 1$ polinomnak nincs többszörös tényezője $\mathbb{Z}_p[x]$-ben (lásd 3.6.7. Gyakorlat). Így $\varphi(m) = 1$, ahonnan (a B.0.7. Állítás szerint) $m = 1$ vagy 2.

3.9.20. Még a primitív

```
with(numtheory):
for n from 3 by 2 do
  if issqrfree(n) and not isprime(n) then
    s := coeffs(cyclotomic(n,x));
    for i in s do
      if i > 4 or i < -4 then
        print(n, sort(cyclotomic(n,x)));
        break
      fi
    od
  fi
od;
```

MAPLE-program is gyorsan kiszámolja a mai asztali számítógépeken, hogy a legkisebb n az $1785 = 3 \cdot 5 \cdot 7 \cdot 17$, melyre Φ_n-ben van legalább 5 abszolút értékű együttható. Az $n = 385 = 5 \cdot 7 \cdot 11$ a legkisebb olyan érték, melyre Φ_n-ben előfordul legalább 3 abszolút értékű együttható, és $n = 1365 = 3 \cdot 5 \cdot 7 \cdot 13$ esetén fordul elő először legalább 4 abszolút értékű együttható.

A szükséges előismeretek összefoglalása

A. ANALÍZIS

A.0.1. Tétel. *Ha f valós együtthatós polinom, akkor a hozzá tartozó $f^* : \mathbb{R} \to \mathbb{R}$ polinomfüggvény folytonos.*

A.0.2. Tétel [Bolzano tétele]. *Legyen f folytonos függvény az $[a, b]$ zárt intervallumon. Ha $f(a) < 0$ és $f(b) > 0$, akkor van olyan $a < c < b$, melyre $f(c) = 0$.*

A.0.3. Lemma. *Legyen f valós együtthatós polinom, melynek főegyütthatója pozitív. Ekkor van olyan c valós szám, hogy $x > c$ esetén $f(x) > 0$ (azaz „elég nagy" x értékekre $f(x)$ már pozitív lesz).*

Bizonyítás. Legyen $f(x) = a_0 + \cdots + a_n x^n$, ahol $a_n > 0$. A háromszög-egyenlőtlenséget (1.4.2. Tétel) felhasználva $x \geq 1$ esetén

$$|a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}| \leq \big(|a_0| + \cdots + |a_{n-1}|\big) x^{n-1} .$$

Ez kisebb, mint $a_n x^n$, ha még

$$x > \big(|a_0| + \cdots + |a_{n-1}|\big)/a_n$$

is teljesül. Ezért az ilyen x-ekre $f(x) > 0$. □

Az alábbi tételt érdemes összevetni a 3.3.8. Tétellel, és az azt követő megjegyzésekkel.

A.0.4. Tétel. *Páratlan fokú valós együtthatós polinomnak van valós gyöke.*

Az algebra alaptételétől független bizonyítás. Mivel f-nek és $-f$-nek ugyanazok a gyökei, feltehetjük, hogy f főegyütthatója pozitív. Az előző lemma szerint f felvesz pozitív értéket. Most tekintsük a $-f(-x)$ polinomot. Mivel f páratlan fokú, ennek a főegyütthatója szintén pozitív. Az előző lemma szerint van olyan d valós szám, hogy $-x > d$ esetén $-f(-x) > 0$. Vagyis x helyébe $-x$-et írva $x < -d$ esetén $f(x) < 0$. Beláttuk tehát, hogy f pozitív és negatív értéket is felvesz, és így Bolzano tétele miatt van valós gyöke. □

B. SZÁMELMÉLET

Az alábbiakban emlékeztetünk néhány olyan számelméleti definícióra és tételre, amelyet a könyvünkben felhasználunk. Általános hivatkozásként Freud Róbert és Gyarmati Edit [**4**] könyvét ajánljuk. Elsőként az Euler-függvénnyel kapcsolatos tudnivalókat foglaljuk össze.

B.0.5. Definíció. Ha n pozitív egész, akkor a $\varphi(n)$ *Euler-függvény* a $0, 1, \ldots, n-1$ számok közül az n-hez relatív prímek száma.

B.0.6. Tétel. *Az Euler-függvény multiplikatív, azaz ha n és m relatív prím pozitív egészek, akkor $\varphi(nm) = \varphi(n)\varphi(m)$. Innen következik, hogy ha n kanonikus alakja $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, ahol egyik α_i kitevő sem nulla, akkor*

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \ldots \left(p_k^{\alpha_k} - p_1^{\alpha_k - 1}\right).$$

Elemi számelméleti okoskodásokkal adódik a fenti képletből az alábbi két állítás, amit a könyvben felhasználunk.

B.0.7. Állítás. *Legyen n pozitív egész.*

(1) *A $\varphi(n)$ értéke akkor és csak akkor* 1, *ha $n = 1$ vagy $n = 2$.*
(2) *A $\varphi(n)$ értéke akkor és csak akkor páratlan, ha $n = 1$ vagy $n = 2$.*

Azt, hogy az Euler-függvény multiplikatív, most be fogjuk bizonyítani, mert a bizonyításból egy olyan összefüggés adódik, amire szükségünk lesz. Ehhez emlékeztetjük az olvasót néhány definícióra. A 2.2. Szakaszban láttuk, hogy amikor a $0, 1, \ldots, n-1$ számokkal modulo n végezzük a műveleteket, akkor egy $\mathbb{Z}_n$ egységelemes gyűrűt kapunk, amelynek az invertálható elemei pontosan azok a $0 \leq i < n$ számok, amelyek n-hez relatív prímek. Ezeknek a halmazát $\mathbb{Z}_n^\times$-tel jelöltük. Vagyis $\mathbb{Z}_n^\times$ elemszáma pontosan $\varphi(n)$. A $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ az olyan (a, b) rendezett párok halmazát jelöli, amelyekre $a \in \mathbb{Z}_n^\times$ és $b \in \mathbb{Z}_m^\times$. Ennek a halmaznak az elemszáma tehát $\varphi(n)\varphi(m)$.

B.0.8. Tétel. *Tegyük fel, hogy n és m relatív prím pozitív egészek. Ekkor létezik olyan $g : \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \to \mathbb{Z}_{nm}^\times$ kölcsönösen egyértelmű megfeleltetés, hogy tetszőleges $a, a' \in \mathbb{Z}_n$ és $b, b' \in \mathbb{Z}_m$ esetén*

$$g(a *_n a', b *_m b') = g(a, b) *_{mn} g(a', b').$$

(ebben a képletben $*_n$ a modulo n szorzás műveletét jelöli, lásd 1.1.1. Definíció). Speciálisan $\varphi(nm) = \varphi(n)\varphi(m)$.

Bizonyítás. Kényelmesebb a g megfeleltetés f inverzét megkonstruálni. Ha $c \in \mathbb{Z}_{nm}^{\times}$, akkor vegyük a c szám n-nel való osztási maradékát, ezt jelölje a. Hasonlóképpen legyen b a c szám m-mel való osztási maradéka, és $f(c) = (a, b)$.

A definíció szerint $0 \leq a < n$. Megmutatjuk, hogy a és n relatív prímek. Valóban, ha volna egy $d > 1$ közös osztójuk, akkor $a \equiv c\ (n)$ miatt d osztaná c-t is, ami lehetetlen, mert c és nm relatív prímek. Ezért $a \in \mathbb{Z}_n^{\times}$. Ugyanígy adódik, hogy $b \in \mathbb{Z}_m^{\times}$. Az f tehát a $\mathbb{Z}_{nm}^{\times}$ halmazt a $\mathbb{Z}_n^{\times} \times \mathbb{Z}_m^{\times}$ halmazba képzi. Ahhoz, hogy belássuk, hogy bijektív, meg kell mutatnunk, hogy f szürjektív és injektív.

Legyen $(a, b) \in \mathbb{Z}_n^{\times} \times \mathbb{Z}_m^{\times}$, és tekintsük az

$$\left.\begin{aligned} x &\equiv a\ (n) \\ x &\equiv b\ (m) \end{aligned}\right\}$$

szimultán kongruenciarendszert. Ennek a kínai maradéktétel szerint van megoldása, és ez egyértelmű modulo nm. Ezért pontosan egy olyan c megoldás van, amelyre $0 \leq c < nm$. Belátjuk, hogy $c \in \mathbb{Z}_{nm}^{\times}$, azaz hogy $(c, nm) = 1$. Tegyük fel ennek ellenkezőjét. Ekkor van olyan q prím, melyre $q \mid c$ és $q \mid nm$. Ezért vagy $q \mid n$, vagy $q \mid m$. Az első esetben $c \equiv a\ (n)$ miatt $q \mid a$ is teljesül, azaz q közös osztója a-nak és n-nek. Ez lehetetlen, mert $a \in \mathbb{Z}_n^{\times}$, azaz $(a, n) = 1$. A második esetben, amikor $q \mid m$, a $(b, m) = 1$ feltétellel kerülünk ellentmondásba. Tehát tényleg $c \in \mathbb{Z}_{nm}^{\times}$. A maradékos osztás egyértelműsége miatt $f(c) = (a, b)$. Tehát f tényleg szürjektív.

Az, hogy f injektív, a kínai maradéktétel egyértelműségi állításából következik. Ha ugyanis $f(c) = f(c') = (a, b)$, akkor c is és c' is megoldása a fenti szimultán kongruenciarendszernek. Tehát $c \equiv c'\ (nm)$. Mivel $0 \leq c, c' < nm$, ezért $c = c'$. Tehát f bijektív, és ezzel φ multiplikativitását beláttuk.

Definiáljuk a g függvényt az f inverzének. Ha tehát $g(a, b) = c$ és $g(a', b') = c'$, akkor $f(c) = (a, b)$ és $f(c') = (a', b')$. Szeretnénk kiszámítani $f(c *_{nm} c')$ értékét, azaz a $c *_{nm} c'$ szám maradékát modulo n és modulo m. A modulo nm szorzás definíciója az, hogy az egész számok között kiszámított szorzatot még redukálni kell modulo nm. Így viszont $c *_{nm} c' \equiv cc'\ (n)$ is teljesül, tehát elegendő a cc' maradékát kiszámolni. Tudjuk, hogy $c \equiv a\ (n)$ és $c' \equiv a'\ (n)$, ezért $cc' \equiv aa\ (n)$. Így cc' maradéka ugyanaz, mint aa' maradéka, azaz $a *_n a'$. Hasonló számolással kapjuk, hogy $c *_{nm} c'$ mod m vett maradéka $b *_m b'$. Tehát $f(c *_{nm} c') = (a *_n a', b *_m b')$. Másképp fogalmazva $g(a *_n a', b *_m b') = c *_{nm} c'$, és ezzel az állítást beláttuk. □

B.0.9. Definíció. A $\mu(m)$ *Möbius-függvényt* a következőképpen definiáljuk: ha az m pozitív egész szám s darab különböző prím szorzata, akkor $\mu(m) = (-1)^s$, egyébként pedig $\mu(m) = 0$.

Természetesen $\mu(1) = (-1)^0 = 1$, hiszen az 1 nulla darab prím szorzata (üres szorzat). A Möbius-függvény egy fontos tulajdonságát fogalmazza meg a következő állítás.

B.0.10. Állítás. *Tetszőleges m pozitív egészre*

$$\sum_{d|m} \mu(d) = \begin{cases} 1 & \text{ha } m = 1, \\ 0 & \text{ha } m \neq 1. \end{cases}$$

Bizonyítás. Az állítás $m = 1$ esetén nyilvánvaló. Tegyük fel, hogy $m > 1$, és legyenek $p_1, \ldots, p_s$ az m szám különböző prímosztói. A $\mu(d)$ értéke 0, kivéve ha d különböző prímek szorzata, azaz $p_1 \cdot \ldots \cdot p_s$ egy rész-szorzata. Ha páratlan sok prímet szorzunk össze, akkor $\mu(d) = -1$, ha páros sokat, akkor $\mu(d) = 1$. Vagyis a fenti összeg értéke akkor lesz nulla, ha a $\{p_1, \ldots, p_s\}$ halmaznak ugyanannyi páratlan elemű részhalmaza van, mint páros elemű. Ez $s \geq 1$ (vagyis $m > 1$) esetén igaz, hiszen a páros elemszámú részhalmazok száma

$$\binom{s}{0} + \binom{s}{2} + \binom{s}{4} + \ldots,$$

a páratlanoké

$$\binom{s}{1} + \binom{s}{3} + \binom{s}{5} + \ldots,$$

viszont a binomiális tétel szerint

$$\binom{s}{0} - \binom{s}{1} + \binom{s}{2} - \binom{s}{3} + \binom{s}{4} - \binom{s}{5} + - \cdots = (1-1)^s = 0\,.$$

□

C. KOMBINATORIKA

C.0.11. Tétel. *Ha van n tárgyunk, akkor ezeket*

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n = \prod_{i=1}^{n} i$$

különböző módon tudjuk sorba rakni. Az itt szereplő $n!$ szám neve: n faktoriális. *Megállapodás szerint $0! = 1$ (lásd a 2.2.23. Gyakorlatot).*

C.0.12. Tétel. *Ha van n tárgyunk, és ebből k darabot akarunk kiválasztani (a sorrendre való tekintet nélkül), akkor ezt*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!}$$

különböző módon tehetjük meg. Az itt szereplő kifejezés az „n alatt a k” binomiális együttható. *Megállapodás szerint ennek értéke nulla, ha $k > n$, vagy ha $k < 0$.*

D. LINEÁRIS ALGEBRA

D.0.13. Definíció. *Vandermonde-determinánsnak* nevezzük az alábbi determinánst:

$$V(z_1,\dots,z_n)=\begin{vmatrix} z_1^{n-1} & \dots & z_n^{n-1} \\ \vdots & \dots & \vdots \\ z_1 & \dots & z_n \\ 1 & \dots & 1 \end{vmatrix},$$

továbbá az ebből transzponálással, valamint a sorok (oszlopok) sorrendjének megfordításával kapható determinánsokat is.

D.0.14. Tétel. *A fenti Vandermonde-determináns értéke*

$$\prod_{1\le i<j\le n}(z_i-z_j)\,.$$

D.0.15. Tétel [A determinánsok szorzástétele]. *Ha M és N azonos méretű, négyzetes mátrixok, akkor* $\det(MN)=\det(M)\det(N)$.

D.0.16. Tétel. *Ha T test, $M\in T^{m\times m}$, $N\in T^{n\times n}$, $X\in T^{n\times m}$, O az $m\times n$-es nullmátrix, akkor*

$$\det\begin{pmatrix} M & O \\ X & N \end{pmatrix}=\det(M)\det(N)\,.$$

A transzponált determinánsra vonatkozó tétel miatt az állítás akkor is igaz, ha a nullák nem a jobb fölső, hanem a bal alsó sarokban vannak.

Ezt az állítást a legegyszerűbb m szerinti indukcióval, az első sor szerinti kifejtéssel igazolni. Következik azonban a determináns Laplace-féle kifejtéséből is.

E. A KÖROSZTÁSI POLINOMOK TÁBLÁZATA

A 3.9. Szakasz feladataiban a Φ_n körosztási polinom kiszámítását visszavezettük arra az esetre, amikor $n > 1$ páratlan, négyzetmentes, nem prím egész szám. Most az ilyen indexű körosztási polinomokat soroljuk fel, $n \leq 105$-ig bezárólag.

$$\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

$$\Phi_{21} = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{33} = x^{20} - x^{19} + x^{17} - x^{16} + x^{14} - x^{13} + x^{11} - x^{10} + x^9 - x^7 + x^6 - x^4 + \\ + x^3 - x + 1$$

$$\Phi_{35} = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + \\ + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1$$

$$\Phi_{39} = x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} + x^{12} - x^{10} + \\ + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{51} = x^{32} - x^{31} + x^{29} - x^{28} + x^{26} - x^{25} + x^{23} - x^{22} + x^{20} - x^{19} + x^{17} - x^{16} + x^{15} - \\ - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{55} = x^{40} - x^{39} + x^{35} - x^{34} + x^{30} - x^{28} + x^{25} - x^{23} + x^{20} - x^{17} + \\ + x^{15} - x^{12} + x^{10} - x^6 + x^5 - x + 1$$

$$\Phi_{57} = x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{29} + x^{27} - x^{26} + x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - \\ - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$$

$$\Phi_{65} = x^{48} - x^{47} + x^{43} - x^{42} + x^{38} - x^{37} + x^{35} - x^{34} + x^{33} - x^{32} + x^{30} - x^{29} + x^{28} - \\ - x^{27} + x^{25} - x^{24} + x^{23} - x^{21} + x^{20} - x^{19} + x^{18} - x^{16} + x^{15} - x^{14} + x^{13} - \\ - x^{11} + x^{10} - x^6 + x^5 - x + 1$$

$$\Phi_{69} = x^{44} - x^{43} + x^{41} - x^{40} + x^{38} - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + \\ + x^{26} - x^{25} + x^{23} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + \\ + x^9 - x^7 + x^6 - x^4 + x^3 -$$

$$\Phi_{77} = x^{60} - x^{59} + x^{53} - x^{52} + x^{49} - x^{48} + x^{46} - x^{45} + x^{42} - x^{41} + x^{39} - x^{37} +$$
$$+ x^{35} - x^{34} + x^{32} - x^{30} + x^{28} - x^{26} + x^{25} - x^{23} + x^{21} - x^{19} + x^{18} - x^{15} +$$
$$+ x^{14} - x^{12} + x^{11} - x^{8} + x^{7} - x + 1$$

$$\Phi_{85} = x^{64} - x^{63} + x^{59} - x^{58} + x^{54} - x^{53} + x^{49} - x^{48} + x^{47} - x^{46} + x^{44} - x^{43} +$$
$$+ x^{42} - x^{41} + x^{39} - x^{38} + x^{37} - x^{36} + x^{34} - x^{33} + x^{32} - x^{31} + x^{30} - x^{28} +$$
$$+ x^{27} - x^{26} + x^{25} - x^{23} + x^{22} - x^{21} + x^{20} - x^{18} + x^{17} - x^{16} + x^{15} -$$
$$- x^{11} + x^{10} - x^{6} + x^{5} - x + 1$$

$$\Phi_{87} = x^{56} - x^{55} + x^{53} - x^{52} + x^{50} - x^{49} + x^{47} - x^{46} + x^{44} - x^{43} + x^{41} - x^{40} +$$
$$+ x^{38} - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + x^{27} - x^{25} + x^{24} - x^{22} +$$
$$+ x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^{9} - x^{7} + x^{6} - x^{4} +$$
$$+ x^{3} - x + 1$$

$$\Phi_{91} = x^{72} - x^{71} + x^{65} - x^{64} + x^{59} - x^{39} - x^{36} + x^{33} -$$
$$- x^{29} + x^{26} - x^{22} + x^{20} - x^{15} + x^{13} - x^{8} + x^{7} - x + 1$$

$$\Phi_{93} = x^{60} - x^{59} + x^{57} - x^{56} + x^{54} - x^{53} + x^{51} - x^{50} + x^{48} - x^{47} + x^{45} - x^{44} +$$
$$+ x^{42} - x^{41} + x^{39} - x^{38} + x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{28} + x^{27} - x^{25} +$$
$$+ x^{24} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^{9} - x^{7} +$$
$$+ x^{6} - x^{4} + x^{3} - x + 1$$

$$\Phi_{95} = x^{72} - x^{71} + x^{67} - x^{66} + x^{62} - x^{61} + x^{57} - x^{56} + x^{53} - x^{51} + x^{48} - x^{46} +$$
$$+ x^{43} - x^{41} + x^{38} - x^{36} + x^{34} - x^{31} + x^{29} - x^{26} + x^{24} - x^{21} + x^{19} - x^{16} +$$
$$+ x^{15} - x^{11} + x^{10} - x^{6} + x^{5} - x + 1$$

$$\Phi_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} +$$
$$+ x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} +$$
$$+ x^{12} - x^{9} - x^{8} - 2x^{7} - x^{6} - x^{5} + x^{2} + x + 1$$

Tárgymutató

Irodalom

[1] Czédli Gábor, B. Szendrei Mária, Szendrei Ágnes: *Absztrakt algebrai feladatok*. Polygon kiadó, Szeged, 2003.

[2] D. K. Fagyejev, I. Sz. Szominszkij: *Felsőfokú algebrai feladatok.* TypoTEX kiadó, 2000.

[3] Freud Róbert: *Lineáris Algebra*. ELTE Eötvös kiadó, Budapest, 1996.

[4] Freud Róbert, Gyarmati Edit: *Számelmélet*. Nemzeti Tankönyvkiadó, Budapest, 2000.

[5] Fried Ervin: *Algebra I.* Nemzeti Tankönyvkiadó, Budapest, 2000.

[6] Fried Ervin: *Algebra II.* Nemzeti Tankönyvkiadó, Budapest, 2002.