Mat-tanári gyakorlat, második évfolyam, második félév
Tizedik alkalom — megoldásvázlatok

1. A faktorgyűrűben reprezentánsokkal számoljunk. A mellékosztályokat az összeadás, nem a szorzás szerint kell képezni, például a $\mathbb{Z}_8/\{0,4\}$ faktorgyűrű elemei $\{0,4\}$, $\{1,5\}$, $\{2,6\}$, $\{3,7\}$. Vigyázzunk, míg csoportok esetében két mellékosztály komplexusszorzata egy teljes mellékosztály volt, addig gyűrűkben két mellékosztály komplexusszorzata általában csak részhalmaza lesz egy mellékosztálynak. Például az iménti példában $\{0,4\}$ önmagával vett komplexusszorzata a $\{0\}$ halmaz, a faktorgyűrűben viszont ennek az elemnek az önmagával vett szorzata $0\cdot 0+\{0,4\}$, azaz önmaga. *A feladat eredménye:* az első három gyűrű $\mathbb{Z}_4$-gyel izomorf. A következő kettő egymással izomorf, de $\mathbb{Z}_4$-gyel nem, mert nem egységelemesek. Az utolsó két gyűrű izomorf.

2. Ha az $\mathbb{R}[x]/(x^2+1)$ faktorgyűrűben akarunk számolni, akkor minden osztályból egy „ügyes" reprezentánst kell kiválasztani. Nyilván f és g akkor és csak akkor van egy osztályban, ha $f-g\in(x^2+1)$, azaz ha f és g ugyanazt a maradékot adja x^2+1-gyel osztva. A lehetséges osztási maradékok éppen az $ax+b$ alakú polinomok, ahol $a,b\in\mathbb{R}$. Két ilyet úgy kell összeszorozni, hogy a szorzást elvégezzük $\mathbb{R}[x]$-ben, és a szorzatnak megkeressük a reprezentánsát, azaz a vele egy maradékosztályban levő $ax+b$ alakú polinomot. Ez persze éppen a szorzatnak az x^2+1-gyel vett osztási maradéka lesz. *Összefoglalva:* ha az $ax+b$ alakú polinomokkal modulo x^2+1 számolunk, akkor éppen az $\mathbb{R}[x]/(x^2+1)$-gyel izomorf gyűrűt kapunk. Ha tehát $\overline{ax+b}=ax+b+(x^2+1)$ jelöli $ax+b$ maradékosztályát, akkor $\overline{ax+b}\cdot\overline{cx+d}=\overline{acx^2+(ad+bc)x+bd}=\overline{ac(x^2+1)}+\overline{(ad+bc)x+ad-bc}=\overline{(ad+bc)x+ad-bc}$. Ezt a komplex számok szorzásával összevetve azonnal látjuk, hogy az $\overline{ax+b}\leftrightarrow ai+b$ megfeleltetés izomorfizmus $\mathbb{R}[x]/(x^2+1)$ és $\mathbb{C}$ között. Speciálisan tehát az i az $\overline{x}=x+(x^2+1)$-hez, az a valós szám pedig az $\overline{a}=a^*=a+(x^2+1)$ maradékosztályhoz tartozik.

Hogy jön ki ez az izomorfizmus a homomorfizmus-tételből? Tekintsük azt az $\mathbb{R}[x]\to\mathbb{C}$ homomorfizmust, amely az f polinomhoz $f(i)$-t rendeli. Ennek képe a teljes $\mathbb{C}$, hiszen minden $ai+b$ szám megkapható például az $ax+b$ polinom képeként. Magja azokból az f polinomokból áll, amik a nullába képződnek, azaz amiknek gyöke az i. Ezek éppen az i minimálpolinomjának többesei. De i minimálpolinomja x^2+1, így a mag (x^2+1).

3. Modulo x^2+x+1 kell számolni az $ax+b$ alakú polinomokkal, ahol $a,b\in\mathbb{Z}_2$. Tehát négy polinomról van szó, legyen $N=\overline{0}=0+(x^2+x+1)$, $E=\overline{1}=1+(x^2+x+1)$, $A=\overline{x}=x+(x^2+x+1)$ és $B=\overline{x+1}=x+1+(x^2+x+1)$. Például $AB=\overline{x^2+x}=\overline{x^2+x+1+1}=\overline{1}=E$ (hiszen minden elem kétszerese nulla). A táblák:

$+$	N	E	A	B
N	N	E	A	B
E	E	N	B	A
A	A	B	N	E
B	B	A	E	N

$*$	N	E	A	B
N	N	N	N	N
E	N	E	A	B
A	N	A	B	E
B	N	B	E	A

Testet kaptunk, mert az E egységelem a szorzástábla minden sorában szerepel az elsőt kivéve. Nyilván $\{N,E\}=\{0^*,1^*\}$ a $\mathbb{Z}_2$-vel izomorf résztest. Az $f(x)=x^2+x+1$ polinomba nem tudunk A-t helyettesíteni, de a neki megfelelő $f^*(x)=Ex^2+Ex+E$ polinomba igen, és láthatjuk, hogy ennek gyökei A és B. Mivel f^* irreducibilis $\{N,E\}$ felett (másodfokú, és nincs e testben gyöke), ezért f^* az A és B minimálpolinomja. Az E minimálpolinomja $Ex-E$, az N-é Ex. Az E elemet 1-gyel, N-et 0-val azonosítva mondhatjuk, hogy $\mathbb{Z}_2$ egy olyan négyelemű, másodfokú bővítését konstruáltuk meg, amelyben az x^2+x+1-nek már van gyöke.

4. a) Az $\mathbb{R}[x]/(x^2-1)$ nem nullosztómentes, mert $x+1+(x^2-1)$ és $x-1+(x^2-1)$ egyike sem nulla (miért?), de szorzatuk az. Ezért e faktorgyűrű nem lehet testtel izomorf. Az $\mathbb{R}[x]/(x^2+2)$ vizsgálatához a 2. feladat mintájára olyan homomorfizmust kell konstruálni, mely az x^2+2 polinomot viszi nullába. Ilyen az $i\sqrt{2}$ behelyettesítése, tehát az $f\mapsto f(i\sqrt{2})$ leképezés. A kép most is a teljes $\mathbb{C}$, hiszen $ai+b$ megkapható $a/\sqrt{2}x+b$ képeként. A mag az $i\sqrt{2}$ minimálpolinomja által generált főideál, azaz (x^2+2). b) A keresett homomorfizmus a $\varphi:\mathbb{Q}[x]\to\mathbb{R}$, ahol $\varphi(f)=f(\sqrt{2})$. c) Itt $\sqrt[3]{2}$-t kell helyettesíteni. d) Rendeljük hozzá minden polinomhoz a konstans tagjának a paritását. Ez homorfizmus $\mathbb{Z}[x]$-ből $\mathbb{Z}_2$-re, és így $\mathbb{Z}[x]/I\cong\mathbb{Z}_2$, ahol I ennek a homomorfizmusnak a magja. Tehát I azokból a polinomokból áll, melyek konstans tagja páros.

5. Az $f(x)x\equiv 1\ (x^2+x+1)$ kongruenciát kell megoldani $f(x)$-re. Használhatnánk a szokásos, euklideszi algoritmuson alapuló eljárást, de most látszik, hogy $f(x)=-x-1$ megoldás. Ezért $x+(x^2+x+1)$ (egyértelmű) inverze $-x-1+(x^2+x+1)$.