1. Lineáris Algebra gyakorlat (2009/2010 ősz)

Néhány megoldás

4. (a) Mindenekelőtt vegyük észre, hogy $0+0=0$, így $a\cdot 0 = a\cdot(0+0) =^{\text{diszt.}} (a\cdot 0)+(a\cdot 0)$ és adjunk mindkét oldalhoz $-(a\cdot 0)$-t: $0 = a\cdot 0$.

(b) Azt kell belátnunk, hogy $(-a)\cdot b$ az $a\cdot b$ ellentetje: $((-a)\cdot b)+(a\cdot b) =^{\text{diszt.}} ((-a)+a)\cdot b = 0\cdot b =^{(a)} 0$.

(c) Tegyük fel, hogy $a\cdot b = 0$. Ha $a\neq 0$, akkor szorozzuk mindkét oldalt a^{-1}-gyel balról: $a^{-1}\cdot(a\cdot b) = a^{-1}\cdot 0$, vagyis $(a^{-1}\cdot a)\cdot b = 0$, amiből $1\cdot b = 0$, $b=0$.

5. Azt kell csak észrevenni, hogy mivel koordinántánként végezzük a műveleteket, ezért az azonosságokat is elég koordinántánként ellenőrizni, vagyis a valós számokra, amikről tudjuk, hogy igazak. Például az összeadás asszociativitása: $\big((a_1,a_2)+(b_1,b_2)\big)+(c_1,c_2) = (a_1+b_1,a_2+b_2)+(c_1,c_2) = ((a_1+b_1)+c_1,(a_2+b_2)+c_2) = (a_1+(b_1+c_1),a_2+(b_2+c_2)) = (a_1,a_2)+(b_1+c_1,b_2+c_2) = (a_1,a_2)+\big((b_1,b_2)+(c_1,c_2)\big)$.

A nullelem nyilván $(0,0)$, az egységelem $(1,1)$.

6. Legyen $T\subseteq\mathbb{R}$ egy test. T-nek van null- és egységeleme: 0_T és 1_T. A nullelem tulajdonsága szerint $0_T+1_T=1_T$, ezért $0_T=0$. Mivel $1_T\cdot 1_T = 1_T$, ezért $1_T=1$.

Ekkor $-1\in T$ is teljesül, hiszen ugyanarra a nullelemre és összeadásra nézve kell ellentettnek lennie mint $\mathbb{R}$-ben, amiből már könnyen látszik, hogy $\mathbb{Z}\subseteq T$, hiszen 1-eseket és -1-eseket összeadhatunk tetszőlegesen sokszor.

Ha $n\in\mathbb{Z}\backslash\{0\}$, akkor $\frac{1}{n}\in T$ is teljesül, hiszen ugyanarra az egységelemre és szorzásra nézve kell inverznek lennie mint $\mathbb{R}$-ben, amiből minden $n,k\in\mathbb{Z}\backslash\{0\}$-ra $\frac{k}{n}\in T$, vagyis $\mathbb{Q}\subseteq T$.

9. Mindenekelőtt vegyük észre, hogy mindig elég maradékokkal számolni, vagyis ha a maradéka p-vel osztva a', $a=kp+a'$, hasonlóan $b=\ell p+b'$, akkor ab maradéka ugyanaz, mint $a'b'$ maradéka p-vel osztva hiszen $=(kp+a')(\ell p+b') = k\ell p^2+a'kp+b'\ell p+a'b'$.

Ebből már szinte minden azonosság következik: a műveletek asszociativitása és kommutativitása, illetve a disztributivitás. Például $(a+_p b)\cdot_p c$ nyilván az $(a+b)\cdot c$ szám p-vel vett maradéka, hiszen ha csak a maradékra vagyunk kiváncsiak, akkor nyugodtan kiszámolhatjuk előbb $a+b$ maradékát és elég azt szorozni c-vel, sőt c maradékával, mert a többi tag ami keletkezne ugyis oszthatő p-vel. Hasonlóan $(a\cdot_p c)+_p(b\cdot_p c)$ az $(a\cdot c)+(b\cdot c)$ szám p-vel vett maradéka. ($+_p$ és $\cdot_p$ a modulo p műveleteket jelöli.)

A nullelem nyilván 0, az egységelem 1, továbbá egy a elem ellentetje $p-a$ (0-nak 0).

Már csak az inverz létezését kell ellenőriznünk. Legyen $a\in\mathbb{Z}_p\backslash\{0\}$. Vizsgáljuk meg a következő számokat: $0\cdot a$, $1\cdot a$, $2a$, $3a$, $\ldots$, $(p-1)a$. Elég belátnunk, hogy páronként különböző maradékot adnak p-vel osztva, mert akkor mivel p darab van belőlük, ezért valamelyikük maradéka 1. És persze ha ka maradéka 1, akkor $k\cdot_p a = 1$.

Tegyük fel, hogy ia és ja ugyanazt a maradékot adja p-vel osztva. Ekkor p osztja $ia-ja = (i-j)a$-t. Mivel p nem osztja a-t ezért osztja $i-j$-t (p prím), de $-p<i-j<p$, ezért $i-j=0$, így $i=j$.