Algebra, syksy 1999, kotitehtävät 11, ratkaisuja

1. Ytimen muodostavat luvun n monikerrat, ts. $\ker f = n\mathbf{Z}$, sillä $f(kn) = (kn) \bmod n = 0$.
Isomorfialauseen mukaan $\mathbf{Z}/(\ker f) \cong \mathbf{Z}/(n\mathbf{Z}) \cong \mathbf{Z}_n$.
Tekijäryhmän alkioita ovat sivuluokat $(\ker f) + a$, esimerkiksi
$(\ker f) + 0 = \ker f = n\mathbf{Z} = \{\dots, -3n, -2n, -n, 0, n, 2n, 3n \dots\}$,
$(\ker f) + 1 = \{\dots, -3n+1, -2n+1, -n+1, 1, n+1, 2n+1, 3n+1 \dots\}$, jne.

2. Tunnetusti $(\mathbf{Z}_n, +_n)$ on Abelin ryhmä. Kertolasku modulo n on suljettu joukossa $\mathbf{Z}_n$, lisäksi se on liitännäinen ja vaihdannainen. Osittelulait: todistetaan tässä vain eka (lisää perustelut):

$$\begin{aligned} a *_n (b +_n c) &= a *_n \big((b+c) \bmod n\big) = \Big(a\big((b+c) \bmod n\big)\Big) \bmod n = \Big(\big(a \bmod n\big)\big((b+c) \bmod n\big)\Big) \bmod n \\ &= \big(a(b+c)\big) \bmod n = (ab+ac) \bmod n = (ab \bmod n) +_n (ac \bmod n) = (a *_n b) +_n (a *_n c). \end{aligned}$$

3. (i) Operaatiot $+$ ja $\cdot$ ovat selvästi laskutoimituksia joukossa $\mathbf{R}^2$.
(ii) Yhteenlaskun neutraalialkio on $(0, 0) \in \mathbf{R}^2$.
(iii) Jos $(x, y) \in \mathbf{R}^2$, niin vasta-alkio $-(x, y) = (-x, -y) \in \mathbf{R}^2$.
(iv)-(v) Selvästi $+$ on liitännäinen ja vaihdannainen.
Täten tämä $(\mathbf{R}^2, +)$ on Abelin ryhmä.
(vi) Kertolasku on liitännäinen, sillä

$$\begin{aligned} (a,b) \cdot \big((c,d) \cdot (e,f)\big) &= (a,b) \cdot (ce-df, cf+de) \\ &= (a(ce-df) - b(cf+de), a(cf+de) + b(ce-df)) \\ &= (ace-adf-bcf-bde, acf+ade+bce-bdf), \\ \big((a,b) \cdot (c,d)\big) \cdot (e,f) &= (ac-bd, ad+bc) \cdot (e,f) \\ &= ((ac-bd)e - (ad+bc)f, (ac-bd)f + (ad+bc)e) \\ &= (ace-bde-adf-bcf,\ acf-bdf+ade+bce) \end{aligned}$$

(vii) Osittelulait:

$$\begin{aligned} (a,b) \cdot \big((c,d) + (e,f)\big) &= (a,b) \cdot (c+e, d+f) \\ &= (a(c+e) - b(d+f), a(d+f) + b(c+e)) \\ &= (ac+ae-bd-bf, ad+af+bc+be), \\ \big((a,b) \cdot (c,d)\big) + \big((a,b) \cdot (e,f)\big) &= (ac-bd, ad+bc) + (ae-bf, af+be) \\ &= (ac-bd+ae-bf, ad+bc+af+be). \end{aligned}$$

4. a) $\mathbf{Z}$ varustettuna tavallisella yhteenlaskulla on tunnetusti Abelin ryhmä. Tämä kertolasku $ab := 1$ on selvästi laskutoimitus (tulos on aina $1 \in \mathbf{Z}$), samoin se on liitännäinen ja vaihdannainen. Riittää siis tarkistaa osittelulain voimassaolo.
Mutta $a(b+c) = 1$ ja $ab + ac = 1 + 1 = 2$, joten ei ole rengas.
b) Jos $ab := 0$ kaikilla $a, b \in \mathbf{Z}$, niin kertolasku on suljettu, liitännäinen ja vaihdannainen (tarkista!). Nyt $a(b+c) = 0$ ja $ab+ac = 0+0 = 0$, joten I osittelulaki on voimassa; toinen seuraa sitten vaihdannaisuudesta. On rengas.

7. (Lause 11.2 kohta 4) Olkoon $a \in R$, $a \neq 0_R$. Nollamatriisista poikkeaville

$$\begin{pmatrix} 0_R & a \\ 0_R & 0_R \end{pmatrix} \begin{pmatrix} a & 0_R \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix} = 0_{M(R)}.$$

5. a) Ks. luennot. b) vaihdannaisuuksia, liitännäisyyksiä eikä osittelulakeja. Mitä pitää testata näkyy ISETL-koodista (voi käyttää myös funktiota `suljettuko`):

```
>  onko_alirengas := func(S,R,s,k);
>>  if is_set(S) then return
>>  (S subset R) and
>>  laskutoimitusko(S,s) and laskutoimitusko(S,k) and
>>  (neutraali(R,s) in S) and
>>  (forall x in S: kaanteis(R,s,x) in S);
>>  end if; end func;
```

c) Totta. Tehtävässä 2 osoitettiin, että $(\mathbf{Z}_n, +_n, *_n)$ todella on rengas. Jos siis $(A, +_n)$ on aliryhmä, niin se on Abelin ryhmä. Kertolaskun on liitännäisyys ja osittelulait periytyvät siis renkaasta. Ainoa ongelma on *onko kertolasku suljettu joukossa* A. Mutta koska yhteenlasku on suljettu ja *kertominen tässä tapauksessa on oikeastaan yhteenlaskua*:

$$a *_n b = (ab) \bmod n = \underbrace{(b + b + b + \ldots + b)}_{a\ kertaa} \bmod n.$$

d) Ei totta, yhteenlaskun neutraalialkiokaan ei kuulu joukkoon! Muttei sen lisääminenkään auta, esimerkiksi

```
>  Z7 := Z(7); s7 := s(7); k7 := k(7);
>  kaikki_aliryhmat(Z7-{0},k7);
{{1}, {1, 6}, {1, 2, 4}, {1, 2, 3, 4, 5, 6}};
```

eikä noista saada nollankaan avulla kuin triviaali alirengas $(\mathbf{Z}_7, +_7, *_7)$.

6. Joukot T_1 ja T_2 ovat alirenkaita, mutta T_3 ei, sillä se ei sisällä edes nollamatriisia (eikä + ole muutenkaan suljettu). Seuraavassa vähän tiivistettyä koodia:

```
>  matrengas(Z3,s3,k3); nimea_rengas(MR,Ms,Mk); #MR;
81;
>  T1 := {[[a,a],[0,0]] | a in Z3}; T1;
{[[0, 0], [0, 0]], [[1, 1], [0, 0]], [[2, 2], [0, 0]]};
>  onko_alirengas(T1,R,Rs,Rk);
true;
>  T2 := {[[a,0],[0,b]] | a,b in Z3}; T2;
{[[0, 0], [0, 0]], [[0, 0], [0, 1]], [[0, 0], [0, 2]], [[1, 0], [0, 0]],
 [[1, 0], [0, 1]], [[1, 0], [0, 2]], [[2, 0], [0, 0]], [[2, 0], [0, 1]],
 [[2, 0], [0, 2]]};
>  onko_alirengas(T2,R,Rs,Rk);
true;
>  T3 := {A | A in R: (exists B in R: A .Mk B = yksi)}; #T3;
48;
>  onko_alirengas(T3,R,Rs,Rk);
false;
>  suljettuko(T3,Ms); suljettuko(T3,Mk);
false; true;
>  T4 := {nolla,yksi,[[2,0],[0,2]]}; T4;
{[[0, 0], [0, 0]], [[1, 0], [0, 1]], [[2, 0], [0, 2]]};
>  onko_alirengas(T4,R,Rs,Rk);
true;
>  T5 := {[[a,b],[0,c]] | a,b,c in Z3}; #T5;
27;
>  onko_alirengas(T5,R,Rs,Rk);
true;
```