Manuel Kauers
RISC-Linz

Hagenberg, December 17, 2002

Computer Algebra Exercises
Solution 1

Ex. (1) Two sets A and B have the same cardinality iff there is a injective map from A to B and another one from B to A. The canonical embedings of $\mathbb{N}$ to $\mathbb{Z}$ and $\mathbb{Q}$ are injective, so it just remains to show that there are also injective maps 1. from $\mathbb{Z}$ to $\mathbb{N}$, and 2. from $\mathbb{Q}$ to $\mathbb{N}$.

1. $\mathbb{Z} \to \mathbb{N}$. Obviously,

$$m\colon \mathbb{Z} \to \mathbb{N}, \qquad m(z) = \begin{cases} 1 & z = 0 \\ 2z & z > 0 \\ 1 - 2z & z < 0 \end{cases}$$

   does the job.

2. $\mathbb{Q} \to \mathbb{N}$. As $\mathbb{Z}$ and $\mathbb{N}$ have the same cardinality, it is sufficient to show that $\mathbb{Q}^+ := \{q \in \mathbb{Q} : q > 0\}$ and $\mathbb{N}$ have the same cardinality. We show that $\mathbb{N}^2$ and $\mathbb{N}$ have the same cardinality, which implies the claim by the canonical (injective) embeding $\mathbb{Q}^+ \hookrightarrow \mathbb{N}^2$.

   Consider

$$q\colon \mathbb{N}^2 \to \mathbb{N}, \qquad q(n,m) = \frac{(n+m+2)\cdot(n+m+1)}{2} - m.$$

   This function is an enumeration of $\mathbb{N}^2$ as might be clarified by the following table where $q(n,m)$ is written down in row n and column m.

1	2	4	7	11	16	22	29	37	46	$\cdots$
3	5	8	12	17	23	30	38	47	57	$\cdots$
6	9	13	18	24	31	39	48	58	69	$\cdots$
10	14	19	25	32	40	49	59	70	82	$\cdots$
15	20	26	33	41	50	60	71	83	96	$\cdots$
21	27	34	42	51	61	72	84	97	111	$\cdots$
28	35	43	52	62	73	85	98	112	127	$\cdots$
36	44	53	63	74	86	99	113	128	144	$\cdots$
45	54	64	75	87	100	114	129	145	162	$\cdots$
55	65	76	88	101	115	130	146	163	181	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Ex. (2) We show that $[0,1) \subseteq \mathbb{R}$ is overcountable (*überabzählbar*) which implies the claim. Using a binary encoding we can identify $[0,1)$ with the set S of all sequences over $\{0,1\}$. Now, assume that S is countable, $S = \{s_1, s_2, s_3, \dots\}$ with

$$\begin{aligned} s_1 &= (s_{11}, s_{12}, s_{13}, \dots), \\ s_2 &= (s_{21}, s_{22}, s_{23}, \dots), \\ s_3 &= (s_{31}, s_{32}, s_{33}, \dots), \\ &\vdots \end{aligned}$$

Consider the sequence

$$\sigma = (\sigma_i)_{i=1}^{\infty}, \qquad \sigma_i = 1 - s_{ii} \quad (i \in \mathbb{N}).$$

Since S is countable and $\sigma \in S$, there must be some $n \in \mathbb{N}$ with $\sigma = s_n$. But then, by definition of σ,

$$s_{nn} = 1 - s_{nn}$$

leads to a contradiction. ■.

Ex. (3) We have to show that $(Q(R), +)$ and $(Q(R), \cdot)$ are abelian groups and that the distributive law holds.

1. $(Q(R), +)$ is an abelian group:

   (a) Associativity:

   $$\begin{aligned} [(a,b) + (c,d)] + (e,f) &= (ad + cb, bd) + (e,f) \\ &= ((ad + cb)f + ebd, bdf) \\ &= (adf + cbf + bde, bdf) \\ &= (adf + b(cf + de), bdf) \\ &= (a,b) + (cf + de, df) \\ &= (a,b) + [(c,d) + (e,f)] \end{aligned}$$

   (b) Commutativity carries over from R,

   (c) The additive unit is $(0,1)$.

   (d) The additive inverse to (a,b) is $(-a,b)$.

2. $(Q(R), \cdot)$ is an abelian group:

   (a) Associativity:

   $$\begin{aligned} [(a,b) \cdot (c,d)] \cdot (e,f) = (ac, bd) \cdot (e,f) = (ace, bdf) &= (a,b) \cdot (ce, df) \\ &= (a,b) \cdot [(c,d) \cdot (e,f)]. \end{aligned}$$

   (b) Commutativity carries over from R.

   (c) The multiplicative unit is $(1,1)$.

   (d) The multiplicative inverse to (a,b) is (b,a).

3. Distributivity:

$$\begin{aligned}[(a,b)+(c,d)]\cdot(e,f) &= (ad+bc,bd)\cdot(e,f) = (ade+bce,bdf)\\ &\sim (adef+bcef,bdf^2) = ((ae)(df)+(bf)(ce),(bf)(df))\\ &= (ae,bf)+(ce,df) = (a,b)(e,f)+(c,d)(e,f).\end{aligned}$$

This complete the proof. ■.

Ex. (4) We claim that $c := \gcd(a,b)$ does the job.

Proof. We have to show that $\langle c\rangle = \langle a,b\rangle$.

"$\subseteq$": Let $z = ma+nb \in \langle a,b\rangle$. Then, as c is the gcd of a and b, there are numbers $a', b' \in \mathbb{Z}$ such that $a = a'c$ and $b = b'c$. Now,

$$z = ma+nb = ma'c+nb'c = (ma'+nb')\cdot c,$$

and hence $z \in \langle c\rangle$.

"$\supseteq$": Let $z = kc \in \langle c\rangle$. According to the extended Euclidean algorithm, there are numbers $s,t \in \mathbb{Z}$ such that $c = sa+tb$. Now,

$$z = kc = k\cdot(sa+tb) = ks\,a+kt\,b,$$

and hence $z \in \langle a,b\rangle$. ■.

To find the special c of $\langle 10982, 55862\rangle$, we have to find the gcd of those numbers. We apply the Euclidean algorithm:

$$\begin{aligned}55862 &= 5\cdot 10982+952\\ 10982 &= 11\cdot 952+510\\ 952 &= 1\cdot 510+442\\ 510 &= 1\cdot 442+68\\ 442 &= 6\cdot 68+34\\ 68 &= 2\cdot 34+0.\end{aligned}$$

We have found that $\gcd(a,b) = 34$, so $\langle 10982, 55862\rangle = \langle 34\rangle$.

Ex. (5)

Proof. I assume $\alpha,\beta \neq 0$. Let $q = \operatorname{pquot}(\alpha a,\beta b)$ and $r = \operatorname{prem}(\alpha a,\beta b)$. Then,

$$\begin{aligned} & & \operatorname{lc}(\beta b)^{m-n+1}(\alpha a) &= q\cdot\beta b+r\\ &\iff & \beta^{m-n+1}\alpha\operatorname{lc}(b)^{m-n+1}a &= \beta q\cdot b+r\\ &\iff & \operatorname{lc}(b)^{m-n+1}a &= \underbrace{\alpha^{-1}\beta^{n-m}q}_{=\operatorname{pquot}(a,b)}+\underbrace{\alpha^{-1}\beta^{n-m-1}r}_{=\operatorname{prem}(a,b)}.\end{aligned}$$

Rearranging terms yields

$$\alpha\beta^{m-n}\operatorname{pquot}(a,b) = \operatorname{pquot}(\alpha a,\beta b)$$

and

$$\alpha\beta^{m-n+1}\operatorname{prem}(a,b) = \operatorname{prem}(\alpha a,\beta b)$$

as desired. ■.