Solutions to odd-numbered exercises
Peter J. Cameron, *Introduction to Algebra*, Chapter 6

6.1 Recall that \(2 = s(s(0))\) and \(4 = s(s(s(0))))\). Now by definition,

\[
\begin{align*}
2 + 2 &= 2 + s(s(0)) \\
&= s(2 + s(0)) \\
&= s(s(2 + 0)) \\
&= s(s(2)) \\
&= 4.
\end{align*}
\]

Not too long; but maybe not enough to satisfy Russell!

6.3 For \(n \geq 1\), let \(n = \{x\}\) (in other words, \(x\) just stands for the string of symbols inside the set brackets for \(n\)). Then \(n + 1 = \{x, \{x\}\}\). So if \(a_n, b_n, c_n, d_n\) denote the numbers of empty set symbols, opening and closing braces, and commas in the string for \(n\), then for \(n \geq 1\)

\[
\begin{align*}
a_{n+1} &= 2a_n, \\
b_{n+1} &= 1 + (b_n - 1) + b_n = 2b_n, \\
c_{n+1} &= (c_n - 1) + c_n + 1 = 2c_n, \\
d_{n+1} &= 2d_n + 1.
\end{align*}
\]

With the initial conditions \(a_1 = b_1 = c_1 = 1, d_1 = 0\), these recurrence relations have the solutions \(a_n = b_n = c_n = 2^n, d_n = 2^n - 1\).

The fact that these expressions are exponentially long indicates why we don’t use them in practice! Our usual decimal system only requires about \(\log_{10} n\) symbols to represent the natural number \(n\).

6.5 Suppose first that \(a > 0\).

Let \(S\) be the set of natural numbers \(n\) such that \(bn > a\). Then \(S\) is non-empty, since for example \(a + 1 \in S\). Also, if \(n \in S\), then clearly \(n + 1 \in S\).

By the Principle of Induction, \(S\) has a least element, say \(m\). We have \(b(m - 1) \leq a\) and \(bm > a\). Putting \(q = m - 1\), we have

\[
bq \leq a < bq + 1,
\]

and subtracting \(bq\) gives \(0 \leq a - bq < b\). Putting \(r = a - bq\), we are done.

Now suppose that \(a < 0\). (In the case \(a = 0\), the result is trivial: \(q = r = 0\).) Then we can find a number \(x\) such that \(a + bx > 0\). [WHY??] By the first part, \(a + bx = bq + r\), where \(0 \leq r < b\); then \(a = b(q - x) + r\).

6.7 Let \(F\) denote the field of fractions of \(E[x]\) (this is the field of rational functions over \(E\)). The evaluation map \(f \mapsto f(a)\) takes \(F\) to \(E(a)\). (This is well-defined. For, if \(p(x)/q(x) \in F\), where \(q\) is a non-zero polynomial, then \(q(a) \neq 0\) since \(a\) is transcendental, so that \(p(a)/q(a)\) is an element of \(E(a)\); moreover, if two expressions \(p(x)/q(x)\)
represent the same element of $F$, then it is clear that the corresponding expressions $p(a)/q(a)$ are equal in $E(a)$.

Moreover, the evaluation map is a homomorphism, and its kernel is zero (since a field has no non-trivial ideals) and its image is $E(a)$ by definition. So it is an isomorphism from $F$ to $E(a)$.

6.9 (a) Suppose that $A$ and $B$ are countable. Then each is bijective with $\mathbb{N}$; that is, we can write $A = \{a_n : n \in \mathbb{N}\}$, and similarly for $B$.

We may assume that $A$ and $B$ are disjoint. For, if $A'$ and $B'$ are sets bijective with $A$ and $B$ which are disjoint, then there is an injection from $A$ to $A \cup B$, and an injection from $A \cup B$ to $A' \cup B'$; so, if $A' \cup B'$ is countable, then so is $A \cup B$ by the Schröder–Bernstein theorem.

A bijection from $\mathbb{N}$ to $A \cup B$ is now given by

$$f(n) = \begin{cases} a_{n/2} & \text{if } n \text{ is even;} \\ b_{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

A bijection between $\mathbb{N}$ and $A \times B$ is harder to write down. We do it by thinking of $A \times B$ written as a square array, and picking up elements on the north-east to south-west diagonals as shown:

\[
\begin{array}{cccc}
(a_0,b_0) & (a_0,b_1) & (a_0,b_2) & (a_0,b_3) \\
(a_1,b_0) & (a_1,b_1) & (a_1,b_2) & (a_1,b_3) \\
(a_2,b_0) & (a_2,b_1) & (a_2,b_2) & (a_2,b_3) \\
(a_3,b_0) & (a_3,b_1) & (a_3,b_2) & (a_3,b_3)
\end{array}
\]

That is, $f(0) = (a_0,b_0)$, $f(1) = (a_0,b_1)$, $f(2) = (a_1,b_0)$, $f(3) = (a_0,b_2)$, ...

(b) By induction from (a), using the fact that $\mathbb{N}^n$ is bijective with $\mathbb{N}^{n-1} \times \mathbb{N}$.

(c) Let $A$ be countable, say (as above) $A = \{a_n : n \in \mathbb{N}\}$. Let $B$ be a subset of $A$, and $S = \{n \in \mathbb{N} : a_n \in B\}$. “Define” a function $\mathbb{N} \to \mathbb{N}$ by letting $f(n)$ be the least element in the set $S \setminus \{f(0), \ldots, f(n-1)\}$. Since any non-empty subset of $\mathbb{N}$ has a least element, this procedure will fail only if $S = \{f(0), \ldots, f(n-1)\}$, in which case $S$ (and hence $B$) is finite. If it never fails, it defines a bijection between $\mathbb{N}$ and $S$, which followed by the map $n \mapsto a_n$ gives a bijection from $\mathbb{N}$ to $B$.

(d) $\mathbb{Z}$ is the union of two clearly countable sets (the natural numbers and their negatives).

We show that the non-negative rationals are countable. Each can be expressed uniquely as a fraction $p/q$ in its lowest terms; thus the non-negative rationals are bijective with a subset of $\mathbb{N} \times \mathbb{N}$, and hence countable by (c). Then $\mathbb{Q}$ is the union of the sets of non-negative and non-positive rationals, each of which is countable.

6.11 Apply Krull’s Theorem to the ring $R/I$, and then use the Second Isomorphism Theorem.
6.13 Let $V$ be a vector space over $F$. Let $\mathcal{B}$ be the collection of all subsets $B$ of $V$ with the property that every finite subset of $B$ is linearly independent. The set $\mathcal{B}$ is ordered by inclusion (that is, $B_1 < B_2$ if $B_1 \subset B_2$).

Let $\mathcal{C}$ be a chain in $\mathcal{B}$, and $C$ its union. Then $C \in \mathcal{B}$. For suppose not; then some finite subset of $C$, say $\{v_1, \ldots, v_n\}$, is linearly dependent. Now each $v_i$ belongs to some member of the chain; say $v_i \in B_{k_i}$. Of the finitely many sets $B_{k_1}, \ldots, B_{k_n}$, one is the largest, say $B_{k_j}$; then $\{v_1, \ldots, v_n\}$ is a linearly dependent finite subset of $B_{k_j}$, contrary to assumption. So $C$ is an upper bound for the chain $\mathcal{C}$ in $\mathcal{B}$.

By Zorn’s Lemma, $\mathcal{B}$ has a maximal element, say $B_0$. We claim that $B_0$ is the required basis. Clearly its finite subsets are linearly independent. Suppose that there is a vector $v \in V$ which is not a linear combination of the vectors in $B_0$. But then $B_0 \cup \{v\} \in \mathcal{B}$, contradicting the maximality of $B_0$. So no such vector can exist.

There is an alternative proof using the Well-ordering Principle and transfinite induction. Well-order the vectors of $V$. Now construct a set $B$ as follows: a vector $v$ is in $B$ if and only if it is not expressible as a linear combination of its predecessors in the order. (Formally, if $B_v$ is the set constructed by stage $v$ of the transfinite induction, then

$$B_v(v) = \begin{cases} B_v & \text{if } v \text{ is a linear combination of vectors in } B_v, \\ B_v \cup \{v\} & \text{otherwise.} \end{cases}$$

Then show that the set so constructed is a basis.)