Corrections to

WHERE DO NUMBERS COME FROM?

The first corrections (even before the book hit the streets) were from Leslie Green. Other corrections came from Maurizio Codogno. I received a long and useful list from Daniel Worrall.

First page of quotations.
Remove stutter in ‘Kroneckecker’ to get Kronecker.

Page 30 one third of the way down. Remove doubled law
The cancellation law for multiplication (see page 15)

Page 30 last displayed formula should read

$$[(1+1),(2+1)] \neq [(2+1),(4+1)]$$

Page 35 Exercise 2.33. Lines labelled (a) and (b) misplaced commas. Should read
(a) If $\mathbf{a} \oplus \mathbf{c} \olessthan \mathbf{b} \oplus \mathbf{c}$, then $\mathbf{a} \olessthan \mathbf{b}$.
(b) If $\mathbf{a} \otimes \mathbf{c} \olessthan \mathbf{b} \otimes \mathbf{c}$, then $\mathbf{a} \olessthan \mathbf{b}$.

Page 35 Exercise 2.33. After lines labelled (a) and (b) add
(c) If $\mathbf{a} \oplus \mathbf{c} = \mathbf{b} \oplus \mathbf{c}$, then $\mathbf{a} = \mathbf{b}$.
(d) If $\mathbf{a} \otimes \mathbf{c} \olessthan \mathbf{b} = \mathbf{c}$, then $\mathbf{a} = \mathbf{b}$.

Page 46 Proof of Theorem 3.2.7 (vii) replace line reading
‘If $a > a'$, the order rule tells us that there exists a natural number c with’
by
‘If $a > a'$, Theorem 2.3.1 (viii) tells us that there exists a positive rational c with’

Page 46 Last line but one. Replace ‘Lemma 1.3.9 (i)’ by ‘Exercise 2.3.3’

Page 47 Proof of Theorem 3.2.7 (xiii). Daniel Worrall points out that this does not work as advertised and suggests the following replacement:-

(xiii) We have $c > c'$ so, by Theorem 2.3.1 (viii), there exists a strictly positive rational k such that $c = c' + k$. We also have $a + b' > a' + b$ so, by Exercise 2.3.3 (xi), it follows that $(a + b')k > (b + a')k$, whence $ak + b'k > bk + a'k$ and $[ak, a'k] \oslash [bk, b'k]$. Thus, using the standard rules for the manipulation of strictly positive rationals given in Theorem 2.3.1,

$$\begin{aligned}\mathbf{a} \otimes \mathbf{c} &= [a, a'] \otimes [c' + k, c'] = \big[(a(c' + k)) + a'c', ac' + (a'(c' + k))\big]\\ &= [ak + (ac' + a'c'), a'k + (ac' + a'c')] = [ak, a'k]\\ &\oslash [bk, b'k] = \big[(b(c' + k)) + b'c', bc' + (b'(c' + k))\big]\\ &= [b, b'] \otimes [c' + k, c'] = \mathbf{b} \otimes \mathbf{c}.\end{aligned}$$

Page 50 Footnote 9. Remove space in Handel's.

Page 51 First paragraph, the name 'del Ferro' has a double r'

Page 56 Proof of Theorem 3.4.10 (ii) Missing 'is'. Should be 'Next we show g is injective'.

Page 58
'Exercise 3.4.2' should be 'Example 3.4.2'

Page 62 Exercise 4.1.3 Replace 'the subtraction rule' by 'the order rule'

Page 70 Definition 4.3.5. 'm divides k' should be 'm divides n'

Page 73 Last sentence of Exercise 4.3.14 replace 'the largest k' by 'the largest $1/k$'.

Page 90 Proof of Lemma 5.2.12 (ii) first line of second displayed equation last bracket wrong size. Should read $(-(2n)) \times (-(2n-1))$

Daniel Worrall points out that Part (ii) of Lemma 5.2.13 is simply wrong. Rewrite as follows

Part (ii) of the next lemma will play a very important role in this chapter.

Lemma 5.2.13

(i) If p is an odd prime and $a \not\equiv 0$, then $a^{(p-1)/2} \equiv 1$ or $a^{(p-1)/2} \equiv -1 \mod p$.

(ii) If p is a prime with $p = 4n + 3$ for some non-negative integer n, then, if $a \equiv b^2 \mod p$, we have $b \equiv a^{(p+1)/4}$ or $b \equiv -a^{(p+1)/4} \mod p$.

Proof. (i) Let $c \equiv a^{(p-1)/2}$. Then, by Fermat's little theorem, $c^2 \equiv a^{p-1} \equiv 1$. Since the equation $x^2 \equiv 1$ has at most two roots, we know that $c \equiv 1$ or $c \equiv -1$ and we are done.

(ii) If $b \equiv 0$, the result is trivial. Otherwise, we know that a has exactly 2 square roots and Fermat's little theorem (Theorem 5.2.1) gives

$$(-a^{(p+1)/4})^2 \equiv (a^{(p+1)/4})^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} \times a \equiv a,$$

as stated. ■

Page 101, start of Proof of Lemma 5.5.1. Omit first two words and comma to get '(i) The equation'

Page 103, second sentence of proof of Lemma 5.5.4. Replace 'Lemma 5.2.13 (iii)' by 'Lemma 5.2.13 (ii)'.

Page 112 Lemma 6.1.3

Last word of proof of Lemma 6.1.3. Replace 'theorem' by 'lemma'.

Page 120 Second line of second paragraph. Insert 'the' to obtain 'obeys the least member principle'

Page 120, line 5, insert 'the'

obeys the least element principle.

Page 127 last line 'shown' should be showed

Page 129

Second paragraph. The general view is that 'self-evident' should be hyphenated. Hyphenate the four instances.

Page 130. In the sentence before Exercise 6.5.3, 'exists she must' should be 'exists must'

Page 138. Omit '(see Theorem 4.4.12)'

Page 146, footnote 14. 'tenth' rather that 'tenths'

Page 147 First sentence of Section 7.3 should end with a full stop and not a comma.

Page 149 Proof of Theorem 7.3.3 (i) Replace 'b_n' by 'a_n' twice

Page 149 Proof of Theorem 7.3.3 (ii) centre of displayed equation. Replace '$|(a - a_n) - (b_n - b)|$' by '$|(a - a_n) + (b_n - b)|$'

Page 153 Proof of Theorem 7.4.8
'Exercise 7.3.4 (i)' should be 'Exercise 7.3.4 (iii)'

Page 156 Proof of Lemma 7.4.12. First part of first sentence
'$f : \mathbb{F} \to \mathbb{F}$' rather than '$f : \mathbb{R} \to \mathbb{R}$'

Page 157 Axiom of dependent choice. Last sentence '$x_1 \in E$' rather than '$x_1 \in S$'

Page 158 Proof of Theorem 7.5.2, last sentence but one.
'$f(a_n) \nrightarrow f(a)$' rather than '$f(a_n) \nrightarrow a$'

Page 157 Footnote 23 Borges's rather than Borge's

Page 163 Proof of Lemma 7.6.12
Replace '$n,\ m > N$' on fourth line by '$n,\ m \geq N$'
Replace '$N(J) > N$' on fifth line by '$N(J) \geq N$'

Page 178 one third down, replace $2S_{n-1} - S_n = 2$ by

$$2S_{n-1} - S_n = 2 - \frac{1}{2^{n-1}} - \frac{1}{2^n}$$

Page 180 Statement of Theorem 8.2.7 ends with full stop not comma.

page 216 line 1 'of' missing. Should be 'construction of $\mathbb{Q}$'

Bibliography. Item [5]
'Brahmegupta' should read 'Brahmagupta'.

****

Finally some typographical errors (offensive to the careful eye but unlikely to cause problems).

Page 24 Top. The formula $4 * 3$ should be $4{*}3$ [Use LaTeX 4{*}3]

Page 45 Two thirds of the way down. Missing space after $\mathbb{Q}^+$.