Errata
Goodman, Algebra: Abstract and Concrete, 2nd ed.

- Page 6: Comments on the paragraph following figure 1.2.5: The "centroid" of the square is the center of mass; it is the intersection of the two diagonals.

  Consider an axis joining two opposite vertices of the square, or the centers of two opposite edges. The figure can be rotated by by 180 degrees (π radians) around such an axis. Such a rotation flips the figure over the axis, exchanging top and bottom. If you flip the figure twice over the same axis, you return it to its original position. It would be convenient to refer to these motions as "flips".

- Page 26: Add two properties to the list of known properties of the integers:
  1. The product of two non-zero integers is non-zero.
  2. For all integers a, b, $|ab| \geq \max\{|a|, |b|\}$.

- Page 35, Exercise 1.6.3: Suppose that the natural number $p > 1$ has the property ...
- Page 38, last line: This shows that (d) implies (a).
- Page 49, proof of 1.8.12: Write $p = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$.
- Page 51, second line of Remark 1.8.17: ... to produce an algorithm ...
- Page 54, exercise 1.8.5: Let h be a non-zero element of $I(f, g)$ of least degree.
- Page 69, Formally, a product or operation on a set G is a function from $G \times G$ to G. For example, the operation of addition on $\mathbb{Z}$ is the function on $\mathbb{Z} \times \mathbb{Z}$ whose value at (a, b) is $a + b$.
- Page 74, Exercise 1.10.9: Show that the set of affine transformations of $\mathbb{R}^n$ ...
- Page 75, Before definition 1.11.1: Again, it is fruitful ...
- The discussion of the RSA algorithm on pages 80-81 is incomplete. Replace Lemma 1.12.1 with the following:

Lemma 1.12.1. *For all integers* a *and* h, *if* $h \equiv 1 \pmod{m}$, *then* $a^h \equiv a \pmod{n}$.

Proof. Write $h = tm + 1$. Then $a^h = aa^{tm}$, so $a^h - a = a(a^{tm} - 1)$. We have to show that $a^h - a$ is divisible by n.

If q does not divide a, then a is relatively prime to q, so $a^{q-1} \equiv 1 \pmod{q}$, by Fermat's little theorem, Proposition **??**. Since $(q - 1)$ divides tm, it follows that $a^{tm} \equiv 1 \pmod{q}$; that is q divides $a^{tm}-1$.

Thus, either q divides a, or q divides $a^{tm} - 1$, so q divides $a^h - a = a(a^{tm} - 1)$ in any case.

Similarly, p divides $a^h - a$. But then $a^h - a$ is divisible by both p and q, and hence by $n = pq = \text{l.c.m.}(p, q)$. ■

Now Lemma 1.12.2 is valid without the hypothesis that a is relatively prime to n. Consequently, in the paragraphs following this lemma, we can eliminate the remark restricting a to be less than n, and the comments about a being relatively prime to n: the procedure is valid for an arbitrary integer a.

- Pages 69-70, We use the notion of a product or operation on a set without defining it. Here is the definition: A *product* or *operation* on a set G is a function from $G \times G$ to G. For example, addition on $\mathbb{Z}$ is the function on $\mathbb{Z} \times \mathbb{Z}$ whose value on the pair $(3, 4)$ is $3 + 4 = 7$.
- Page 88: It would be useful to insert a discussion of the general assocative law here.

Consider a set M with an associative operation, denoted by juxtaposition. The operation allows us to multiply only two elements at a time, but we can multiply three or more elements by grouping them so that only two elements are multiplied at a time. For three elements, there are two possible groupings,

$$a(bc) \quad \text{and} \quad (ab)c,$$

but these are equal by the associative law. Thus there is a well-defined product of three elements, independent of the way in which the three elements are grouped.

There are five ways to group four elements for multiplication,

$$a(b(cd)), \quad a((bc)d), \quad (ab)(cd), \quad (a(bc))d, \quad ((ab)c)d,$$

but by the associative law, the first two and the last two are equal. Thus there are at most three different product of four elements:

$$a(bcd), \quad ,(ab)(cd), \quad (abc)d.$$

Using the associative law, we see that all three are equal:

$$a(bcd) = a(b(cd)) = (ab)(cd) = ((ab)c)d = (abc)d.$$

Thus there is a well-defined product of four elements, which is independent of the way the elements are grouped for multiplication.

There are 14 ways to group five elements for multiplication; we won't bother to list them. Because there is a well-defined product of four or less elements, independent of the way the elements are grouped for multiplication, there are at most four distinct products of five elements:

$$a(bcde), \quad (ab)(cde) \quad (abc)(de), \quad (abcd)e.$$

Using the associative law, we can show that all four products are equal,

$$a(bcde) = a(b(cde)) = (ab)(cde),$$

etc. Thus the product of five elements at a time is well-defined, and independent of the way that the elements are grouped for multiplication.

Continuing in this way, we obtain the following general associative law:

Proposition 2.1.19. *(General associative law) Let M be a set with an associative operation, $M \times M \longrightarrow M$, denoted by juxtaposition. For every $n \geq 1$, there is a unique product $M^n \longrightarrow M$,*

$$(a_1, a_2, \ldots, a_n) \mapsto a_1 a_2 \cdots a_n,$$

such that

(a) *The product of one element is that element $(a) = a$.*
(b) *The product of two elements agrees with the given operation $(ab) = ab$.*
(c) *For all $n \geq 2$, for all $a_1, \ldots a_n \in M$, and for all $1 \leq k \leq n-1$,*

$$a_1 a_2 \cdots a_n = (a_1 \cdots a_k)(a_{k+1} \cdots a_n).$$

Proof. For $n \leq 2$ the product is uniquely defined by (a) and (b). For $n = 3$ a unique product with property (c) exists by the associative law. Now let $n > 3$ and suppose that for $1 \leq r < n$, a unique product of r elements exists satisfying properties (a)-(c). Fix elements $a_1, \ldots a_n \in M$. By the induction hypothesis, the $n-1$ products

$$p_k = (a_1 \cdots a_k)(a_{k+1} \cdots a_n),$$

which involve products of no more that $n-1$ elements at a time, are defined. Moreover, we have $p_k = p_{k+1}$ for $1 \leq k \leq n-2$, since

$$\begin{aligned} p_k &= (a_1 \cdots a_k)(a_{k+1} \cdots a_n) = (a_1 \cdots a_k)(a_{k+1}(a_{k+2} \cdots a_n)) \\ &= ((a_1 \cdots a_k)a_{k+1})(a_{k+2} \cdots a_n) = (a_1 \cdots a_{k+1})(a_{k+1} \cdots a_n) \\ &= p_{k+1}. \end{aligned}$$

Thus all the products p_k are equal, and we can define the product of n elements satisfying (a)-(c) by

$$a_1 \cdots a_n = a_1(a_2 \cdots a_n).$$

■

- Page 89: Omit Exercise 2.1.4.
- Page 89: Exercise 2.1.5 should refer to Proposition 2.1.5, not 2.1.6.
- Page 99, Corollary 2.2.28: Let $b \in \mathbb{Z}$, $b \neq 0$.

- Page 102, Exercise 2.1.14: ... the orders $o(a)$ and $o(b)$ of a and b are relatively prime.
- Page 105, before Figure 2.3.4: the co-ordinates of the vertices are $\begin{bmatrix} \cos(2k\pi/n) \\ \sin(2k\pi/n) \\ 0 \end{bmatrix}$ for $k = 0, 1, \ldots, n-1$.
- Page 113, Comment on Proposition 2.4.12: We remind the reader that if $f : X \longrightarrow Y$ is any map, and $B \subseteq Y$, then $f^{-1}(B)$ denotes the pre-image of B in X, namely $f^{-1}(B) = \{x \in X : f(x) \in B\}$. This alwasy makes sense even if f does not have have an inverse function, and the notation is not supposed to suggest that f has an inverse function.

  In Proposition 2.4.12, we consider a homomorphism $\varphi : G \longrightarrow H$ between groups. For a subgroup $B \subseteq H$, $\varphi^{-1}(B)$ means the set of elements $g \in G$ such that $\varphi(g) \in B$.
- Page 125, three lines from the bottom: Each left coset is nonempty ...
- Page 139, Proof of Proposition 2.7.12, second paragraph. There is a missing bar over over G in the second line. The paragraph should read:

  To prove (b), we show that the map $A \mapsto \varphi(A)$ is the inverse of the map $\overline{B} \mapsto \varphi^{-1}(\overline{B})$. If $\overline{B}$ is a subgroup of $\overline{G}$, then $\varphi(\varphi^{-1}(\overline{B}))$ is a subgroup of $\overline{G}$, that a priori is contained in $\overline{B}$. But since φ is surjective, $\overline{B} = \varphi(\varphi^{-1}(\overline{B}))$.
- Page 143, Exercise 2.7.5 should read:

  Suppose G is a finite group. Let N be a normal subgroup of G and A an arbitrary subgroup. Verify that

$$|AN| = \frac{|A|\,|N|}{|A \cap N|}.$$

- Page 144, Exercise 2.7.7, Part (a): Show that $\mathrm{Aut}(G)$ is a group.
- Page 146, Example 3.1.3: Let a and b be relatively prime natural numbers, each greater than 1.
- Page 151, Exercise 3.1.7 should be skipped; it is the same as Proposition 3.1.4.
- Page 154, Exercise 3.2.1: ... is the inverse of (n, a).
- Page 157, proof of Lemma 3.3.3, first line: Let b_1 be any element of G such that ...
- Page 158, Proof of Proposition 3.3.4, 3rd paragraph, second line: Thus, $g - \sum_{i \geq 2} n_i a_i \in A_1 = \langle a_1 \rangle$, so ...

- Page 159, proof of Theorem 3.3.8, 2nd paragraph, 3rd line: Consider the homomorphism $\varphi(x) = px$ of G into itself.

- Page 160, statement of Lemma 3.3.11: Suppose a finite abelian group G is an internal direct product of a collection $\{C_i\}$ of cyclic subgroups, each of order a power of a prime.

- Page 221, Example 5.4.14. There is an error in the argument in the second paragraph. The third Sylow theorem does not imply that the subgroups Q and R are normal. Instead, one must argue that at least one of the subgroups Q and R must be normal. The argument is as follows:

  By the third Sylow theorem, the number n_5 of conjugates of R is congruent to 1 (mod 5), and divides 30. Hence $n_5 \in \{1, 6\}$. LIkewise the number n_3 of conjugates of Q is congruent to 1 (mod 3) and divides 30. Hence $n_r \in \{1, 10\}$. I claim that at least one of Q and R must be normal. If R is not normal, then R has 6 conjugates. The intersection of any two distinct conjugates is trivial (as the size must be a divisor of the prime 5). Therefore, the union of conjugates of R contains $6 \times 4 = 24$ elements of order 5. Likewise, if Q is not normal, then the union of its 10 conjugates contains 20 elements of order 3. Since G has only 30 elements, it is not possible for both R and Q to be non-normal.

  Since at least one of R and Q is normal, $N = RQ$ is a subgroup of G of order 15. Now N is normal in G, since it has index 2, and cyclic, since any group of order 15 is cyclic.

- Page 222, Exercise 5.4.2: This is just plain wrong. Who knows what I was thinking!

- Page 229, In the description of the polynomial rings over a ring R, one should require that the ring R have a multiplicative identity. (There is a way to get around this requirement, but it is not important to do so at this point.)

- Page 232, Example 6.1.9. Same comment here. One should require that R have an identity.

- Page 232, Example 6.1.9, third line: R[[x]], instead of K[[x]].

- Page 233, Exercise 6.1.2: Assume the ring R has identity element.

- Page 234, Exercise 6.1.17: Consider only the situation that R has an identity element.

- Page 236, Corollary 6.2.6, 2nd line of statement: ... that extends ψ.

- Page 236, Corollary 6.2.6: I should not mention the kernel of $\tilde{\psi}$ here, as the notion of kernel is defined only on the next page. The

statement about the kernel is repeated on the next page in Example 6.2.13.

- Page 238, Example 6.2.15 and Definition 6.2.16: RxR is supposed to denote

$$\{\sum_i r_i x r_i' : r_i, r_i' \in R\},$$

rather than

$$\{rxr' :, r, r \in R\}.$$

The latter set is not closed under addition, and therefore not an ideal, in general.

- Page 424, Definition E.2: A set S of vectors is ...
- Page 428, Definition E.9: The *range* of a linear transformation $T : V \to K^m$ is $\{T(\mathbf{x}) : \mathbf{x} \in V\}$.
- Page 430, proof of Lemma E.15, last line: Hence the span of $S \backslash \{\boldsymbol{\nu}_j\}$ is the same as the span of S.
- Page 431, 4th line from bottom: A matrix M has a left inverse ...
- Page 433, twice on the page: Cauchy-Schwarz rather than Cauchy-Schwartz.