Remarks and Errata to "A Concrete Introduction to Higher Algebra", 3rd edition, 2009, by Lindsay N. Childs, published by Springer-Verlag New York (first edition, 1979, second edition, 1995).

My thanks to Ted Turner and Marco Varisco of Albany, Herb Enderton of UCLA, Keith Conrad and John Watterlond of the Univ. of Connecticut, John McKay of Concordia, Dmitry Gokhman of the Univ. of Texas at San Antonio, Dr. Andrew Mauer-Oats of Evanston Township High School, Julian Wilson of the Hanze Institute of Technology (Groningen), David Marshall of Monmouth Univ., UAlbany students Heather Cavelius, Anh Ngoc Le, Matt Patrick and Yueyi Zheng, reviewers Ken Brown (MR) and Rade Dimitric (ZB), and especially Axel Boldt of Metropolitan State Univ. (Saint Paul, MN) for providing errata and comments for this edition. Errors that if unnoticed could lead to significant confusion are starred.

• p. x, line -2: "A course in Number Theory could follow chapters..." (Rade Dimitric)

• p. 6, line 3: $b \neq 0$ should be $n \neq 0$. Axel Boldt suggests that standard properties of divisibility should be recorded: if $a|b$ and $b|c$, then $a|c$; if $a|b$ and $a|c$ then $a|(rb + sc)$ for all integers r, s; if $a|b$ then $a|bc$; if $a|b$ and $b|a$ then $a = \pm b$; $1|a$, $a|0$, if $a|b$ then $|a| \leq |b|$ (all easy consequences of the definition).

• p. 16, line 3: "$n \geq n_0$" (Axel Boldt)

• p. 16, paragraph above Proposition 4. Divisibility should be defined for integers, not just for natural numbers. (Axel Boldt)

• p. 20. Theorem 8 should read "Any non-empty set of non-negative integers has a least element": it is used in that form in the proof of the Division Theorem in Section 3A. Of course if well-ordering is true for non-empty sets of natural numbers, then well-ordering is also true for any non-empty set S of integers bounded below by some fixed integer b (take the set $T = \{s + 1 - b | s \text{ in } S\}$: then T is a non-empty set of natural numbers.) (Axel Boldt)

• *p. 27, in the Division Theorem, replace "$q > 0$" by "$q \geq 0$". (Ted Turner) . The Division Theorem is also true for b any integer: Given integers $a > 0$ and b, there exist integers q and r with $0 \leq r < a$ such that $b = aq + r$. The more general version is implicitly used in Chapter 5, Exercise 1. (Axel Boldt)

• p. 35, Section C, line 4: Euclid of course assumed that $1 \leq a < b$. (Axel Boldt)

• p. 44, Proposition 10. Since Theorem 5 (Bezout's identity) was only proven for $a, b > 0$, Proposition 10 should read, "Given numbers

a, b, c, there are integers m and n with $am + bn = e$ if and only if (a, b) divides e." The proof was a bit sloppy with notation. Preferable is: "Conversely, if $d = (a, b)$ divides e, then by Bezout's Identityh we can find integers r, s so that $ar + bs = d$. If $e = dt$ for some integer t, then $m = rt, n = st$ satisfies $am + bn = e$. " In the subsequent examples, x and y are unknowns, and letters between a and t are integers. (Axel Boldt)

• p. 45, line 6: "Or if we want to solve $35 = 365x + 1876y$, we may notice ..." (Axel Boldt)

• p. 54, proof of Theorem 2. Axel Boldt observed that n is used both as a number to be factored, and as the number of prime factors in a factorization of n. So suppose $a = p_1 \cdots p_l$ everywhere in the proof, rather than $a = p_1 \cdots p_n$.

• p. 56, Exercise 5. Replace "$< \sqrt{n}$" by "$\leq \sqrt{n}$". (The square of a prime is a counterexample to $<$.) (Dmitry Gokhman)

• p. 72. Proposition 1 is true when $m = 1$, and is also true for every integer, not just every natural number: that is the content of Exercise 1 on page 73.

• *pp. 78-79. In example 6, replace the number 3589 by 3489 everywhere, and on page 79, line 11, adjust the congruence accordingly by replacing 5 by 4. (Ken Brown ("the Glasgow one"))

• p. 85, lines 5 and 8 of Section F. To be completely clear, one should note that given the integers c, d, a, b and $m > 0$, we are solving the congruences for x.

• p. 87, Example 10. Axel Boldt suggests replacing this example because the inverse of 9 is 9. So consider

$$14x \equiv 12 \pmod{20}.$$

Cancel 2 from everything (how can you do that?) to get

$$7x \equiv 6 \pmod{10}.$$

The inverse of 7 modulo 10 is 3, so multiply by 3 to get

$$3 * 7x \equiv 3 * 6 \pmod{10};$$

reducing modulo 10 gives

$$x \equiv 8 \pmod{10}$$

so $x \equiv 8$ or $18 \pmod{20}$.

• *p. 113, Exercise 54, the domain of the function f_b should be $\mathbb{Z}/m\mathbb{Z}$. The function may be one-to-one on U_m even if b is not a unit, as Dmitry Gokhman pointed out–for example, $m = 6, b = 2$. It is a nice problem to try to find all moduli m for which there exists a non-unit b so that f_b is one-to-one on U_m.

• p, 121, line 20: "1194673 is a multiple of 53, 1194689 is a multiple of 23, ..."

• p. 121, line -9: "In Chapter 10 we will give a method..."

• p. 127, line-6. In view of the condition that in a field, $0 \neq 1$, it could be noted that $\{0\}$ is a commutative ring (with the only possible addition and multiplication).

• p. 128, Theorem 1. Axel Boldt suggests mentioning again that addition and multiplication of congruence classes is well-defined, as was shown on pages 96-97. As he aptly notes, well-defined is "a concept that students struggle with".

• p. 130, line 3. We should also note that $a - b$ means $a + (-b)$.

• *p. 130. Exercises 1, 2, 6 and 7 are out of order. The first exercise should be Exercise 7: $b \cdot 0 = 0$. This, along with the uniqueness of negatives, is needed to prove that $-a = (-1)a$, which, in turn, is helpful for doing Exercises 1, 2, and 6. (My students tend to assume both $b \cdot 0 = 0$ and $-a = (-1)a$ to do those exercises.) Axel Boldt also observed that on page 144 we use $-0 = 0$, which follows immediately from Exercise 7 and $-a = (-1)a$.

• p. 131, line -2: $= (A^2 + 0) - B^2$ (Axel Boldt)

• p. 137, Theorem 12: (i), (ii) and (iii) are "if and only if", not just "if". The "only if" follows from Theorem 14: every non-zero element of $\mathbb{Z}/m\mathbb{Z}$ is either a unit or a zero divisor, and Proposition 11: no element of $\mathbb{Z}/m\mathbb{Z}$ can be both a unit and a zero divisor. (Axel Boldt)

• *p. 138, line 4. "Theorem 6" should be "Theorem 12". (Herb Enderton)

• p. 138, Proof of Theorem 14. Axel Boldt suggests that the formula $a^r \cdot a^d = a^{r+d}$ should be proven by induction.

• p. 140. It would be appropriate to define a subring of a ring , and to observe that if $f : R \to S$ is a ring homomorphism, then the image $f(R)$ is a subring of S. (Axel Boldt)

•p. 142, line -11. $f(0) = 0_R$ is required by property (iv). (Herb Enderton)

• p. 143, proof of Proposition 18: Axel Boldt accurately observes that this is just a sketch of a proof, and as such only for $m, n > 0$. A full proof would use induction to justify properties (ii) and (iii) and would need to deal also with negative integers m and n.

• p. 145, Example 7. Extending Axel Boldt's comment for page 140, it would be useful to observe here that for a homomorphism $f : \mathbb{Z} \to R$, the image $f(\mathbb{Z})$ is a subring of R. In case R is a field, the homomorphism f is used on page 144 to define the characteristic of the field. If the characteristic is $p \neq 0$, then the image of f is the prime

subfield of R, isomorphic to $\mathbb{F}_p$. This fact is explicitly used on page 499.

• *p. 146, line 2, $\mathbb{Z}//6\mathbb{Z}$ should be $\mathbb{Z}/6\mathbb{Z}$. (Herb Enderton)

• *p. 165-6, Example 4 is totally defective, since the matrix A has determinant 0 modulo 26. (John McKay)

• p. 172, proof of Proposition 1, one could justify the canceling of a^s by citing Chapter 5, Proposition 17.

• p. 172, line -8. Rade Dimitric complained about the statement, "the notion of order is similar to that of least common multiple". Perhaps I should have explained better what I meant. The order of an element of a finite group and the least common multiple of two numbers are both least elements of non-empty sets of natural numbers. The existence of each is known from the well ordering principle. In practice, to find the least common multiple of b and c, it doesn't suffice to find a common multiple m of b and c – we must also check that m is the least number that is a common multiple of b and c. Similarly, to find the order of an element a, it doesn't suffice to find an exponent $e > 0$ so that $a^e = 1$ – we must also check that e is the least positive integer so that $a^e = 1$. Students sometimes forget to check the leastness when looking for the order of an element.

• p. 174, Exercise 8, line 2: "and the order of a modulo s...": the "a" should be in italics. (Herb Enderton)

• p. 178, Exercise 33: $U(1)$ should be $U(p)$. (Marco Varisco)

• p. 189, proof of Proposition 11. As Axel Boldt observed, this proof is a nice application of Chapter 4, Corollary 3 (if a prime p divides ab it must divide a or b) and Chapter 3, Corollary 8 (if a divides bc and is coprime to b, then a divides c).

•p. 194, lines 2, 12, 13: replace 179 by 177: we expand the exponent $177 = 128 + 32 + 16 + 1$, not the modulus 179. (Herb Enderton). Also line -2 should end with a^{177}, not a^{101}. (Axel Boldt)

• p. 201, line 7: L Adleman (1977) should be L. Adleman (1978) (Marco Varisco)

• *p. 202, lines 11, 15: the equalities should be congruences mod m. (Herb Enderton)

• p. 207, line -9: either delete "n divides" or make it read "verify that n divides $2^{n-1} - 1$, then..." (Marco Varisco)

• p. 225, line 4 of the proof of Theorem 1. "all the elements of aG are distinct". (Axel Boldt)

• p. 227, Section B, line 6: "H is a subset of G which is closed under products and inverses in G, and hence is a group itself under those operations."

• p. 228, line -5. One should note that the usual laws of exponents are valid: for all integers m, n, we have$(a^n)^m = a^{nm}, a^n * a^m = a^{n+m}, (a^{-1})^m = a^{-m}$, and, if a and b commute, then $(ab)^m = a^m * b^m$. (Axel Boldt)

• p. 233. Exercise 16 should read in part: "... to write down the cosets of the subgroup...".

• *p. 235. Exercise 21 should read: "Show that every element $[a]$ in the coset $[b](U_m)(m-1)$ satisfies $[a]^{m-1} = [c]$." (Anh Ngoc Le)

• *p. 238, Exercise 27, (ii). Since 14 is not coprime to 35, the solutions to x^2 congruent to 14 modulo 35 are not units, so do not lie in a coset of $H = U_{35}(2)$. But this is an instructive error. Since 14 is congruent to 49 modulo 35, two solutions to the congruence are $x = 7$ and -7 modulo 35. (One can show, using the Chinese Remainder Theorem, that those are the only solutions of the congruence.) Now if one looks at the "coset" $[7]H$, one finds that $[7]H = [7], [7], [-7], [-7]$, hence contains only two elements of $\mathbb{Z}/35\mathbb{Z}$, not four elements. Critical to the proof of Lagrange's Theorem is the result that every coset bH of a subgroup H of G contains the same number of elements as H. This example shows that if one is too casual about what is meant by a "coset", then that result is false.

• p. 241, Insert just above Proposition 15. "If there is an isomorphism between G and G', we sometimes denote that by writing $G \cong G'$. We'll set some examples of isomorphic groups in Section H. " After Proposition 15 insert. "We will see examples of Proposition 15 in Section 12D–in particular, see Proposition 8. "

• p. 244, line 4. "To do this, we let $G = U_p$ and let $N = \{1, -1\}$, a subgroup of G (where we write..."

• p. 245, line 5. Note that H is a subgroup of G by Exercise 35 on page 242.

• p. 245, line -16. Perhaps one should recall from page 233 that the order of an element of a group divides the order of the group.

• p. 246, Example 24. It might be helpful to recall Exercise 33 of Chapter 7: the only integers n with $n^2 \equiv 1 \pmod{p}$ are $n = 1$ and -1. (Axel Boldt)

• *p. 247, line 5. "the left coset $a * H$ and the right coset $H * a$ are equal." (Ken Brown)

• *p. 254. In the EEA matrix for solving $74r - 63s = 2$, the row containing 66 should contain 6 and -6. (Yueyi Zheng)

• p. 273, line -11: "as noted in the following exercises." (Marco Varisco)

• p. 275, rewrite Proposition 4. "Let $\gamma_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be as above. If g is a ring homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to S, then the composition

$f = g\gamma_m$ is the unique ring homomorphism from $\mathbb{Z}$ to S, and the kernel of f contains $m\mathbb{Z}$. " This wording avoids the inappropriate term "lifts".

• p. 275, line -13. The reader could be reminded that the ordered pair notation (r, s) here has nothing to do with the greatest common divisor of two numbers. (Axel Boldt)

• p. 276-277. The reader should note that in notation such as (0, 1) in Example 13, the left 0 is the zero element of $\mathbb{Z}/2\mathbb{Z}$ and the right 1 is the multiplicative identity element of $\mathbb{Z}/3\mathbb{Z}$. (Axel Boldt)

• p. 277, line 13. "The proof of Theorem 7 relates to the Chinese Remainder Theorem" (Herb Enderton)

• p. 286, line 11. Since $\mathbb{Q}[x]$ isn't defined until the next page, this line should be rewritten as "Thus if $p(x) = 3x^2 - 2x + 5$, a polynomial with coefficients in the rational numbers $\mathbb{Q}$, then .... If $p(x) = [3]x + [4]x^3$, a polynomial with coefficients in $\mathbb{Z}/6\mathbb{Z}$, then replacing x by $[2]$ in $\mathbb{Z}/6\mathbb{Z}$..." (Axel Boldt)

• p. 290, line -4. "...in formula (13.2) above. To illustrate..." (Rade Dimitric)

• p. 292, first line of Example 1. "Let $Func(R, R)$ be the ring of functions..." (Herb Enderton)

• *p. 296, line -11. $(x^2 - 1)(x^2 + 1) = x^4 - 1$. (Heather Cavelius)

• *p. 297. In the proof of D'Alembert's Theorem, "We must show $r \leq n$ ... Hence $r \leq n = deg(f)$." (David Marshall)

• p. 298, last line of Exercise 3, add a period before the). (Herb Enderton has sharp eyes for proofreading!)

• *p. 300, second line of Theorem 8: "... written as $d = rf + sg$ for..." (Herb Enderton)

• *p. 305, Exercise 45. "then $f(x)$ has an irreducible factor of degree $\leq n/2$" . (Herb Enderton)

• p. 307, line 12: "we can ask how $x^3 - 2$ factors in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$, and in $\mathbb{C}[x]$." (Axel Boldt)

• p. 307, line 14: In $\mathbb{Q}[x]$, $x^3 - 2$ is irreducible because it has no roots in $\mathbb{Q}$, hence no factor of degree 1. (Axel Boldt)

• p. 309, Theorem 1. The letter r is used for the remainder on line 7, so should preferably not be used as the number of prime factors of g in the theorem. So replace r by k in the statement and proof of Theorem 1 (except in Lemma 2). (Ted Turner)

• *p. 329, line -11: the displayed polynomial should be $p(x) = x^2 - 2ax + (a^2 + b^2)$. (Marco Varisco)

• p. 336, line 6. Section 12E should be section 9E.

• p. 313, line -7. Omit "over any field" (redundant). (Axel Boldt)

• p. 331, line 8, "$|(a_{n-1}|$" should be "$(|a_{n-1}|$". (Axel Boldt)

• p. 346, Proposition 6. Omit the second "for some m" (Axel Boldt)

• p. 346, Example 5. "easily": by Chapter 14, Exercises 45 and 46, one needs only check that x^5+x^2+1 is not divisible in $\mathbb{F}_2[x]$ by $x, x+1$ and x^2+x+1.

• p. 347, line 2 of Example 10: $\Phi(x) = x^{p-1} + x^{p-2} + \dots$. (Marco Varisco)

• p. 347, line 4 of Example 10: the ϕ should be Φ . (Ted Turner)

• p. 355, line 9 should read "if m divides $f-g$". (John Watterlond)

• p. 357, Proof of Proposition 5, line 1: "$f(x)$ by $x-r$" (Axel Boldt)

• *p. 357, line -10 (Example 1). $f(x) = m(x)(x^3+2x^2+2x) + (x+1)$ (an example where detaching the coefficients when dividing polynomials led to error!). (Matt Patrick)

• *p. 363: Exercises 4, 5 and 6 should read "of degree ≤ 1", "of degree ≤ 2", "of degree ≤ 2", respectively.

• p. 369, line 9 of Section D: "Schubert" . (Axel Boldt)

• p. 369, line -12. Choose $n_0, \dots, n_d$ so that the integers $r_0, \dots, r_d$ are all non-zero integers. (Axel Boldt)

• p. 370, Example 9. To check irreducibility of x^4+x+1 in $\mathbb{Z}[x]$, use Chapter 16, Proposition 6 and Chapter 14, Exercise 45. (Axel Boldt)

• p. 379, line -12: "c_{e_1}" should be "c_{e-1}" twice. (Axel Boldt)

• p. 392, Definition. Omit "of order n". (Axel Boldt)

• p. 396, line -4: recall the properties of $\phi(m)$ from Chapter 9, Proposition 7.

• p. 414, line 10: recall Chapter 19, Theorem 12.

• p. 416, line 14. "An idea like this could only..." (Keith Conrad)

• p. 426, Section D (i). Axel Boldt objected to this subsection, because the strong a-pseudoprime test separates composite numbers from primes almost as efficiently as the Fermat test separates composite non-Carmichael numbers from primes and Carmichael numbers. (But I like Proposition 7).

• p. 438, line 12. $\left(\frac{103}{3}\right) = -1$ should be $\left(\frac{3}{103}\right) = -1$. (Axel Boldt)

• *p. 450, Exercise 21: show that $(((p-1)/2)!)^2$ is congruent to $(-1)^{(p-1)/2}$ modulo p. (students of Andrew Mauer-Oats)

• p. 451, line 4: three dots ... are missing in the displayed formula. (Marco Varisco)

• p. 459, line 1 of Proposition 1. Axel Boldt suggested a bit of explanation for the first sentence: since a quadratic residue modulo p is a square modulo p, it must have order dividing $(p-1)/2$.

• p. 463, line 6. Keith Conrad's web page address should start www.math.uconn.edu/ conrad/ ... .

• p. 470, line 18, replace "is is" by "is". (Axel Boldt)

• p. 473, line l6. "Suppose we wish to factor a number N of 100 digits": the "N" should be in italics. (Keith Conrad)

• p. 486, lines 3-7. The manipulations here are justified at the bottom of the page in Section C. (Axel Boldt)

• *p. 489, Example 13 is defective: the first remainder in Euclid's Algorithm is $x^3 + x^2 + x$.

• p. 493, line 1, $E = \mathbb{F}_2[x]/(x^4 + x + 1)$. (Axel Boldt)

• p. 499, line -10, p, 500, lines, 17, 15, 16: "$F[x]/(q(x))$" (Axel Boldt)

• p. 501, Proof of Theorem 6, line 2: "some field K containing $\mathbb{F}_p$" (Axel Boldt)

• p. 514, Table 25.2: $\alpha + 1 = \alpha^4, \alpha^2 + 1 = \alpha^8, \alpha^2 + \alpha = \alpha^6$.

• p. 522, line 6 of "Decoding": " To find $E(x)$, we need to find". (Axel Boldt)

• p. 531, line 2 of Section A. Axel Boldt pointed out correctly that since a polynomial $f(x)$ of degree n has n roots in $\mathbb{C}$, the existence of a bound on the roots of $f(x)$ is obvious. The challenge is to find a good bound on the roots that is efficiently computable from the coefficients of $f(x)$. We found such a bound in Section 15F; in section B we find some better bounds. Theorem 2 on page 532 depends on knowing a bound B that is computable in finitely many steps. (The bound in Section 15F is such a bound.)

• *p. 536, line 14 (last line of the proof): replace r by c: "is < 0 for $0 < x < c$, and is > 0 for $x > c$".

• p. 540, line 13: "with $0 \le k \le d$," (Axel Boldt)

• *p. 544, Theorem 7. "let $h(x)$ in $\mathbb{F}_p[x]$ be a polynomial of degree ≥ 1 and $< d$ such that..." (Axel Boldt)

• *p. 544, line -2. "must involve only polynomials of degree $< d$. (Axel Boldt)

• p. 545, formula (26.1) "...= $h(x^p)$." line -1, "$x^{ip} \equiv r_i(x) \pmod{f(x)}$, and similarly two lines below. (Axel Boldt)

• p. 550, line 17. The theorem used here is not the Interpolation Theorem but the Chinese Remainder Theorem (Chapter 17, Theorem 7). (Axel Boldt)

• p. 553, Proposition 10: "If deg $k <$ deg(gh), then we can..." (Axel Boldt)

• p. 554, line -10: "Since g_1 and h_1 are coprime modulo m ..." (Axel Boldt)

• p. 559, first line of the proof of Proposition 5: "Write $n = p^e q$ with p prime and $e > 0$." (Axel Boldt)

• p. 560, line 6, last sum, omit the first (. (Axel Boldt)

• p. 563, Section B, line 2: replace $\mathbb{Z}_p[x]$ by $\mathbb{F}_p[x]$. (Axel Boldt)

• p. 563, last line, "$nN_n(0) \geq p^n - \sum_{d|n, d<n} p^d$." (Axel Boldt)

• p. 564, Theorem 10. "For every $g \geq 1$ let M_g be the product of the first g odd primes. For every $n \geq 2$, let $I_n(M_g) = ...$" (Axel Boldt)

• p. 565, line 15, omit the period at the end of the display. (Axel Boldt)

• p. 566, line -3 of the proof of Theorem 10: "and so by the Sandwich Theorem for limits," (Axel Boldt)

• p. 569ff. Often the hints refer to parts a), b), ... of an exercise when the reference should be to parts i), ii), ..., for example, for exercise 9 of Chapter 4 (p. 572). (Marco Varisco)

• p. 569, hint for Chapter 1, Exercise 2 d): reflexivity also fails (Julian Wilson)

• *p. 570. The last three hints for Chapter 2 should be for Exercises 36, 37 and 38. (Herb Enderton)

• p. 577, Chapter 9, Exercise 14: the answers to part (ii) is 1 and to part (iii) is 5. (Herb Enderton)

• *p. 578. Chapter 9. The hints on page 578 should be to Exercises 70 (which is correct in the text), 75 (not 71), 76 (not 73), 79 (not 76), 82 (not 80), 85 (not 82), 88 (not 85) and 89 (not 86). (Herb Enderton)

• p. 582, Chapter 14, Exercise 4 (iii): Let $y = x^4$. (Marco Varisco)

• p. 584, Chapter 15, Exercise 42: the proof of Theorem 10 ... applies. (Marco Varisco)

• p. 597, "Lenstra, A. K. and Lenstra, H. W. Jr., The development of the number field sieve ..." (Keith Conrad)

• p. 601, the term "Logarithm table" is on p. 107 and p. 403. (Ted Turner)

• p. 603, the term "Roots of unity" is on page 318 and on p. 347. (Herb Enderton)

Last update, August 7, 2013.