Abstract Algebra, *Second Edition*, by John A. Beachy and William D. Blair

Corrections and clarifications

Note: Some corrections were made after the first printing of the text.

page 9, line 8
For of the form $ma + nb$
read of the form $ma + nb$, where $m, n \in \mathbf{Z}$,

page 22, line -13 (Exercise 17)
For Use Exercise 16
read Use Exercise 15

page 24, line -3
For doing any computations with
read adding, subtracting, or multiplying

page 26, line -13
For has no solution modulo 6.
read has no solution.

page 27, line -8
For the equation $x \equiv cb_1 + mk$
read the equation $x = cb_1 + mk$

page 35, line -6
For there is a unique solution to the congruence $ax \equiv 1 \pmod{n}$,
read any two solutions to $ax \equiv 1 \pmod{n}$ are congruent modulo n,

page 38, line 14
For *Proof.* See Exercises 15 and 27.
read *Proof.* See Exercise 28.

page 48, line -1
For equivalence class
read congruence class

page 54, line 17
For define an inverse $g : S \to T$
read define an inverse $g : T \to S$

page 54, line 19
For $S \times T$
read $T \times S$

page 54, line -12 (Exercise 1) and line -6 (Exercise 2)
For or onto.
read and whether it is onto.

page 56, line 9 (Exercise 17)
Add Let A be a nonempty set.

page 60, line 3 (Definition 2.2.4)
For *subsets of* S
read *nonempty subsets of* S

page 60, line 6
For set S
read nonempty set S

page 63, line -10 (Exercise 11)
For the set S
read the nonempty set S

page 63, line -9 (Exercise 11)
For Example 2.2.6
read Proposition 2.2.5

page 64, line -8
For write $\sigma\tau$.
read write $\sigma\tau$, and refer to this as the *product* of the two permutations.

page 67, line 2
For cycle of length k
read cycle of length $k \geq 2$

page 67, line 3
Add In fact, $(1) = (a)$ for any cycle (a) of length 1.

page 67, line -2
For illustrates
read illustrate

page 70, line 2 (Theorem 2.3.5)
For *The cycles that appear in the product*
read *The cycles of length* ≥ 2 *that appear in the product*

page 70, line -10
Add Note that cycles of length 1 can be omitted.

page 71, line -4
For $\sigma^k(a_1) = a_k$
read $\sigma^k(a_1) = a_{k+1}$

page 76, line -9 (Exercise 10)
For Let τ be the cycle
read Let $\tau \in S_n$ be the cycle

page 76, line -8 (Exercise 10)
For if σ is any permutation,
read if $\sigma \in S_n$,

page 76, line -6 (Exercise 10)
For there exists a permutation σ
read there exists a permutation $\sigma \in S_n$

page 89, line -11
For if and only its
read if and only if its

page 99, line 18
For the stated range
read the stated codomain

page 107, line -7
For **(iii)** $a(b+c) = ab + ac$ *for all* $a, b, c \in F$.
read **(iii)** $a(b+c) = ab + ac$ *and* $(a+b)c = ac + bc$ *for all* $a, b, c \in F$.

page 110, line -11 (Exercise 12)
For It must contain an element of order 2, since the order of G is even.
read Show that G must contain an element of order 2 (see Exercise 21 of Section 3.1).

page 111, line -1
For the first row of the table
read the last row of the table

page 118, line 7
For multiplying both sides of this equation by $(\phi(x_2))^{-1}$ gives us $\phi(x_1x_2^{-1}) = \phi(x_1)(\phi(x_2))^{-1} = e$,
read $\phi(x_1x_2^{-1})\phi(x_2) = \phi(x_1x_2^{-1}x_2) = \phi(x_1) = \phi(x_2) = e\phi(x_2)$, so we can cancel $\phi(x_2)$ to get $\phi(x_1x_2^{-1}) = e$,

page 122, line -5
For since the subgroups can be linearly ordered.
read since for any two subgroups, one is contained in the other. (Why?)

page 126, line 16 (Exercise 19)
For where p is a prime number.
read where p is a prime number, and $k \geq 1$.

page 129, line -4
For the identity $ba = a^2b$.
read the equation $ba = a^2b$.

page 130, line 1 of the text, and again in line 2 of the text
For identity $ba = a^3b$.
read equation $ba = a^3b$.

page 131, line 5 of the text, and again in line 7 of the text
For identity $ba = a^{n-1}b$
read formula $ba = a^{n-1}b$

page 131, line -7
For the identities they satisfy.
read the equations $a^n = e$, $b^2 = e$, and $ba = a^{n-1}b$ that they satisfy.

page 143, lines 2
For the congruence classes of G/ϕ are just the individual elements of G,
read the equivalence classes of G/ϕ are just the subsets of G consisting of single elements,

page 153, line 9
For *The group G is called a* simple *group*
read *The nontrivial group G is called a* simple *group*

page 153, line -3
For identity $ba = a^3b$
read equation $ba = a^3b$

page 155, line -7 (Exercise 7)
For Let H be a subgroup
read Let H be a finite subgroup

page 160, line 4
For $a_1 - a_2 = (b_2 - a_2)\sqrt{2}$, so if $b_2 - a_2 \neq 0$ then we can divide by $b_2 - a_2$,
read $a_1 - a_2 = (b_2 - b_1)\sqrt{2}$, so if $b_2 - b_1 \neq 0$ then we can divide by $b_2 - b_1$,

page 164, line -10
For $x^5 - 2x + 1$ and $4x + 1$ are identical, as functions.
read $x^5 - 2x + 1$ and $4x + 1$ define the same function.

page 165, line 3
For multiplying each term be every other
read multiplying each term by every other

page 175, line 10, following Definition 4.2.3
Add Note that if both $f(x)$ and $g(x)$ are the zero polynomial, then by our definition there is no greatest common divisor.

page 180, line -7 (Exercise 11)
Add (where p is any prime number).

page 182, line -12
For If c is a root of $f(x)$
read If c is an integral root of $f(x)$

page 182, line -6
For rational roots of equations such as
read integer (and thus rational) roots of monic equations such as

page 186, line 7
For $(x^8 - x^7 + x^5 - 2x^4 + x^3 - x + 1)$
read $(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)$

page 187, line -9 (Exercise 9)
For Let m and n are
read Let m and n be

page 191, line -7
For Proposition 4.4.6
read Theorem 4.4.6

page 194, line 1 (Exercise 11)
For Find an irreducible polynomials
read Find an irreducible polynomial

page 199, line 8
For If effect
read In effect

page 211, line 14
For commutative rings
read commutative rings with identity,
For ring homomorphism
read ring homomorphism that preserves the multiplicative identities

page 218, line -12 (Exercise 20)
For with characteristic p
read with characteristic $p > 0$

page 229, line 15
For the sum should be $ab + bc$
read the sum should be $ad + bc$

page 236, line 5
For e and π are transcendental
read e and π are transcendental over $\mathbf{Q}$

page 249, line 3
For Proposition 4.2.1
read Proposition 4.3.1

page 259, line -3 (Theorem 6.6.1)
For *irreducible factors*
read *monic irreducible factors*

page 263, line 7 (Definition 6.6.8)
For *The number of irreducible polynomials*
read *The number of monic irreducible polynomials*

page 270, line -1, and page 271, lines 1, 3, 4
For $\left(\dfrac{3}{p}\right)$
read $\left(\dfrac{p}{3}\right)$

page 274, line 2
For $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_{k-1} \supseteq N_k = \{e\}$
read $G = N_0 \supset N_1 \supset \ldots \supset N_{k-1} \supset N_k = \{e\}$

page 274, line 16
For A nontrivial abelian group
read An abelian group

page 279, line 8 (Exercise 10)
For for all positive integers n.
read for all positive integers $n \geq 3$.

page 281, line -15
For $ab \in G$
read $ab \in C(x)$

page 281, lines -15

For Furthermore, $axa^{-1} = x$ implies that $a^{-1}xa = x$, and then $a^{-1} \in C(x)$ since $a^{-1}x(a^{-1})^{-1} = x$.

read Furthermore, $a^{-1} \in C(x)$, since $axa^{-1} = x$ implies that $x = a^{-1}xa$, and thus $a^{-1}x(a^{-1})^{-1} = x$.

page 285, line -8 (Exercise 10)

For identity $ba = a^{-1}b$. Show that a^m is conjugate to only a^{-m},

read equation $ba = a^{-1}b$. Show that a^m is conjugate to only itself and a^{-m},

page 290, line 4 (Theorem 7.3.8)

For *the number of solutions*

read *the number of solutions in* G

page 296, line -4 (Lemma 7.5.3)

For *maximal cyclic subgroup of* G

read *cyclic subgroup of* G *of maximal order*

page 297, line 6

For maximal cyclic subgroup

read cyclic subgroup of G of maximal order

page 297, line -10

For $\mathbf{Z}_{p^{\alpha_1}} \times \mathbf{Z}_{p^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p^{\alpha_n}} = \mathbf{Z}_{p^{\beta_1}} \times \mathbf{Z}_{p^{\beta_2}} \times \cdots \times \mathbf{Z}_{p^{\beta_m}}$

read $\mathbf{Z}_{p^{\alpha_1}} \times \mathbf{Z}_{p^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p^{\alpha_n}} \cong \mathbf{Z}_{p^{\beta_1}} \times \mathbf{Z}_{p^{\beta_2}} \times \cdots \times \mathbf{Z}_{p^{\beta_m}}$

page 300, line -13 (Lemma 7.5.9)

For *if* n *is a nonnegative integer less than* 2^{k-2}.

read *as* n *ranges over nonnegative integers less than* 2^{k-2}.

page 300, line -4

For $\pm 5^n \pmod{2^k}$, with $m > n$.

read $\pm 5^n \pmod{2^k}$, with $m \geq n$.

page 303, line 16

Add By omitting all unnecessary terms, we can assume that each factor group is nontrivial.

page 305, line 13

For $(G/N)^{(n)} = N$

read $(G/N)^{(n)} = \{N\}$

page 305, line -5

Add *The number of composition factors in a composition series is called the* length *of the series.*

page 307, line -15 (Exercise 4)

For G_i and H_i is simple

read G_i and H_i is a finite simple group

page 307, line -3 (Exercise 6 (d))

For Prove that any normal Sylow p-subgroup

read Prove that if G is finite, then any normal Sylow p-subgroup of G

page 308, line -10
For $d, f \in \mathbf{Z}^+$
read $d, f \in \{1, 2, \ldots, n\}$

page 309, line 15
For In the first case, $\sigma^{-1}\tau\sigma\tau^{-1} = (a, b, d, c, g)$, for $\tau = (b, c, d)$,
read Let $\tau = (b, c, d)$. In the first case, $\sigma^{-1}\tau\sigma\tau^{-1} = (a, b, d, c, g)$,

page 319, line 13 (Lemma 8.1.5)
For *a polynomial with no repeated roots*
read *a polynomial such that each irreducible factor has no repeated roots,*

page 319, line -3 (Theorem 8.1.6)
For *If $f(x)$ has no repeated roots,*
read *If no irreducible factor of $f(x)$ has repeated roots,*

page 332, line -13 (Theorem 8.3.10)
For *Any polynomial*
read *Any nonconstant polynomial*

page 334, line 3
For The subgroup $G_1 = \mathrm{Gal}(F/\mathbf{C})$ of G is also a 2-group, and is normal since it has index 2. Thus F is a normal extension of $\mathbf{C}$, and so we can again apply Theorem 8.2.8. If G_1 is not the trivial group, then the first Sylow theorem implies that it has a normal subgroup N of index 2.
read The subgroup $G_1 = \mathrm{Gal}(F/\mathbf{C})$ of G is also a 2-group. If G_1 is not the trivial group, then the first Sylow theorem implies that it has a normal subgroup N of index 2. Since F is a normal extension of $\mathbf{C}$, we can again apply Theorem 8.3.8.

page 334, line 6
For $[K : \mathbf{C}] = [G : N] = 2$
read $[K : \mathbf{C}] = [G_1 : N] = 2$

page 334, line -3 (Definition 8.4.1)
For $n_1, n_2, \ldots, n_m \in \mathbf{Z}$
read $n_1, n_2, \ldots, n_m \in \mathbf{Z}^+$

page 338, line 16
For It can be shown that the polynomial $f(x) = g(x) - 2$ has exactly two nonreal roots in $\mathbf{C}$, and if k is prime, then the Galois group of $f(x)$ over $\mathbf{Q}$ is S_k.
read The polynomial $f(x) = g(x) - 2$ has exactly two nonreal roots in $\mathbf{C}$, if m is chosen large enough, and if k is prime, then its Galois group over $\mathbf{Q}$ is S_k (see Section 4.10 of Jacobson's *Basic Algebra I*).

page 342, line -9
For α^k must be a root of $f(x)$
read β^k must be a root of $f(x)$

page 343, Example 8.5.2
Note The complete answer to the constructibility question is that a regular n-gon is constructible if and only if $n = 2^k p_2 \cdots p_m$, where $k \geq 0$, and

the factors p_i are distinct Fermat primes. The remarks in Example 8.5.2 indicate a proof of the “only if” part of the condition. See Section 4.11 of Jacobson’s *Basic Algebra I* for the “if” part of the proof.

page 343, line -13
For Wedderburn (1891-1965)
read Wedderburn (1882-1948)

page 346, line 4 (Proposition 8.6.2)
For *roots* $r_1, \ldots, r_n$ *in its splitting field* F.
read $f(x) = p_1(x)p_2(x) \cdots p_k(x)$ *its factorization in* $K[x]$ *as a product of distinct irreducible polynomials. If* F *is the splitting field of* $f(x)$ *over* K,

page 349, line 6
For $\Delta = -4p^3 - 27q^3$.
read $\Delta = -4p^3 - 27q^2$.

page 350, line -6 and page 351, line 2
For (a, d, c, d)
read (a, b, c, d)

page 351, line 10
For with precisely two real roots
read with precisely three real roots

page 351, line 15
For a cyle of the form
read a cycle of the form

page 352, lines 7,8
For Reducing modulo 31, we have the factorization $x^5 - 2x^3 - 8x - 2 = (x^3 + 15x^2 + 4x - 1)(x + 8)^2$.
read Reducing modulo 37, we have the factorization $x^5 - 2x^3 - 8x - 2 = (x^3 - 12x^2 - 11x + 7)(x^2 + 12x + 5)$.

page 352, lines 9
For GF(31)
read GF(37)

page 362, line 16 (Exercise 10)
For is principal,
read has the form aR, for some $a \in R$,

page 363, lines 8 and -13
For $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_1 x + a_0$
read $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

page 364, line 11
For To show uniqueness, suppose that $(a/b)f^*(x) = (c/d)g^*(x)$, where $g^*(x)$ is also primitive. Then $adf^*(x) = bcg^*(x)$, and so the irreducible factors of ad and bc must be the same. Since a and b are relatively prime and D is a unique factorization domain, this implies that a and c are associates and that b and d are also associates. This in turn implies that $f^*(x)$ and $g^*(x)$ are associates.

read To show uniqueness, let $(a/b)f^*(x) = (c/d)g^*(x)$, where $g^*(x)$ is primitive and c and d have no irreducible factors in common. Then $adf^*(x) = bcg^*(x)$, so the irreducible factors of ad and bc must be the same. Since a and b have no irreducible factors in common and D is a unique factorization domain, we see that a and c are associates, and that b and d are associates. Thus $f^*(x)$ and $g^*(x)$ are associates.

page 373, line 3
For $x^3 + 1$
read $x^3 - 1$

page 373, line 4
For $x^3 - 1$
read $x^3 + 1$

page 373, line 12
For the defining identity
read the defining equation

page 393, line -14
For $\overline{(z + w)} = \overline{z} + \overline{w}$ and $\overline{(zw)} = \overline{zw}$.
read $\overline{z + w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$.

page 413, line -3
For $[x + 1]$ | $[0]$ $[x + 1]$ $[x + 1]$ $[x + 1]$
read $[x + 1]$ | $[0]$ $[x + 1]$ $[x + 1]$ $[0]$

Last revision: 2/22/2005