Corrections to
Basic Algebra

Basic Algebra appears in two versions, the original edition of 2006 and a revised edition dated 2015. Most of the corrections to the original edition that are listed below are implemented in the revised edition. In what follows, the short list of corrections to the revised edition appears first, and it is followed by two lists of corrections to the original edition.

Corrections to the Revised Edition

Page 330, last text line before the second displayed equation. Change "$F : G \to C$" to $F : G \to \mathbb{C}$".

Page 334, lines 3–4. Change "$AR(g) = R(xg) = R(gx) = R(g)A$" to "$AR(x) = R(gx) = R(xg) = R(x)A$".

Short Corrections to the Original Edition

Page xii, line 3. Change "University" to "Universal".

Page 3, after the statement of Proposition 1.2c. Insert "Remark. Proposition 1.2c is sometimes called **Bezout's identity**."

Page 5, Lemma 1.6. Insert a remark saying, "Lemma 1.6 is sometimes known as **Euclid's Lemma.**"

Page 7, first paragraph. Change "n'" to "t" in three places.

Page 8, display in Corollary 1.11. Change "$\min_{1\le j\le r}$" to "$\min_{1\le j\le t}$" twice.

Page 15, proof of Proposition 1.20. Replace sentences 3 through 5 with "Since $\lim_{x\to\pm\infty} P(x)/x^{2n+1} = 1$, there is some positive r_0 such that $P(-r_0) < 0$ and $P(r_0) > 0$."

Page 21, line −9. Change "Once" to "In the general case, as soon as".

Page 21, line −6. Change "any of" to "any added variables".

Page 25, line labeled "(c)". Change "$A + (-A) = (-A) + 0$" to "$A + (-A) = (-A) + A = 0$".

Page 34, item after (ii, a). Change "(a) $1v = v$" to "(b) $1v = v$".

Page 39, line before the statement of Theorem 2.6. Change "$\mathbb{R}^k$" to "$\mathbb{F}^k$".

Page 39, first display in the proof of Theorem 2.6. Change "Av_n" at the far right to "c_nAv_n".

Page 40, proof of Theorem 2.8, line 3. Change "To see the middle inequality" to "To see the middle equality".

Page 58. An end-of-proof symbol "□" should be moved from the end of line 9 to the end of line 4.

Page 62, second of the three paragraphs. For clarity, change "direct" to "external direct" in five places in this paragraph only.

Page 66, line above display in the middle of the page. Change "$\det L = \begin{pmatrix} L \\ \Gamma\Gamma \end{pmatrix}$" to "$\det L = \det \begin{pmatrix} L \\ \Gamma\Gamma \end{pmatrix}$".

Page 71, line 4. Change "$(-1)^{l+j} \det \widehat{A_{lj}}$" to "$(-1)^{l+j} A_{lj} \det \widehat{A_{lj}}$".

Page 76, line −8. Change "is an eigenvalue" to "is an eigenvector".

Page 94, next-to-last line. Change "$u'_k = v_k - (v_k, u_1) - \cdots - (v_k, u_{k-1})u_{k-1}$" to "$u'_k = v_k - (v_k, u_1)u_1 - \cdots - (v_k, u_{k-1})u_{k-1}$."

Page 96, line 7. Change "$v_1 = \sum_{i=1}^{r} u_i$" to "$v_1 = \sum_{i=1}^{r} (v, u_i)u_i$", and change "$v_2 = \sum_{j=r+1}^{n} u_j$" to "$v_2 = \sum_{j=r+1}^{n} (v, u_j)u_j$".

Page 104, line 3 of statement of Lemma 3.20. Change "eigenvalues are orthogonal" to "eigenvectors are orthogonal".

Page 125, after proof of Proposition 4.4. Insert "REMARK. The proof of Proposition 4.4 exhibits a one-one correspondence between the subgroups of $\mathbb{Z}/m\mathbb{Z}$ and the positive integers k dividing m."

Page 126, line −2 of the proof of Proposition 4.5. Change "$g_1 g_2 g'_1 g_2$" to "$g_1 g_2 g'_1 g'_2$".

Page 128, line −8. Change "mZ" to "$m\mathbb{Z}$".

Page 129, after the proof of Theorem 4.7. Insert "REMARK. Using the formula in Theorem 4.7 three times yields the conclusion that if H and K are subgroups of a finite group G with $K \subseteq H$, then $|G/K| = |G/H|\,|H/K|$."

Page 133, line 13. Change "that $h_2 h'_2$ and h_2^{-1} are in $\varphi^{-1}(H_2)$" to "that $g_1 g'_1$ and g_1^{-1} are in $\varphi^{-1}(H_2)$".

Page 134, line 6 of proof of Theorem 4.14. Change "$(h_2^{-1} h_1^{-1} h_2) h_2^{-1}$" to "$h_1^{-1}(h_1 h_2^{-1} h_1^{-1})$."

Page 136, Figure 4.2. Change the name of the map on the top arrow from "φ_s" to "φ_{s_0}".

Page 145, line 2 of proof of Proposition 4.20. Change "$(i_1 r_1 + r_1 i_2 + i_1 i_2)$" to "$(i_1 r_2 + r_1 i_2 + i_1 i_2)$".

Page 150, line −16. Change "$R = \mathbb{C}[X]$" to "$R = \mathbb{C}$, $T = \mathbb{C}[X]$,".

Page 152, line 7. Change "p^{r-s}" to "p^{r+s}" in three places.

Page 158, line 3 of Section 6. Change "Examples 5–9 of groups in Section 1 were" to "When $X = \{1, \ldots, n\}$, the group $\mathcal{F}(X)$ is just the symmetric group $\mathfrak{S}_n$. Thus Examples 5–9 of groups in Section 1 are all".

Page 160, line 9. For purposes of this discussion, one may take this displayed equation as a definition of $\mathrm{SU}(1,1)$.

Page 162, line 11. Change "**isotropy subgroup** at p" to "**isotropy subgroup** at p or **stabilizer** of G at p."

Page 162, line 20. Insert a footnote after the clause "If $Y = Gp$ is an orbit". The footnote reads, "Although the notation G_p for the isotropy subgroup and Gp for the orbit are quite distinct in print, it is easy to confuse the two in handwritten mathematics. Some readers may therefore prefer a different notation for one of them. The notation $Z_G(p)$ for the isotropy subgroup is one that is in common use; its use is consistent with the notation for the "centralizer" of an element in a group, which will be defined shortly. Another possibility, used by many mathematicians, is to write $G \cdot p$ for the orbit."

Page 164, last line. Change "$|G| = p^k$" to "$|G_k| = p^k$", and change "$G_k \subseteq G_{k+1}$" to "$G_k \subsetneqq G_{k+1}$".

Page 165, line 3. Change "4.39" to "4.38".

Page 165, proof of Lemma 4.41. Change "n" to "r" in all 5 places it appears in the proof.

Page 166, line −3. Change "$h \to \tau_g(h)$" to "$h \mapsto \tau_g(h)$".

Page 167, line −2. Change "$= (g,h)(g^{-1},1)$" to "$= (g,h)(g,1)^{-1} = (g,h)(g^{-1},1)$".

Page 167, footnote. Add a sentence at the end: "The normal subgroup goes on the open side of the $\ltimes$ and on the side of the subscript τ in $\times_\tau$."

Page 169, line −6. Change "$a^k \to b^{k(q-1)/p}$" to "$a^k \mapsto b^{k(q-1)/p}$".

Page 171, last display. Change "$\{1,\ (1\ 2)\}$" to "$\{1,\ (1\ 2)(3\ 4)\}$".

Page 171, line −5. Change "$\{1,\ (1\ 2)\}$" to "$\{1,\ (1\ 2)(3\ 4)\}$".

Page 171, line −1. Change "$\{1,\ (1\ 2)\}$ by $\{1,\ (1\ 3)\}$ and again by $\{1,\ (1\ 4)\}$" to "$\{1,\ (1\ 2)(3\ 4)\}$ by $\{1,\ (1\ 3)(2\ 4)\}$ and again by $\{1,\ (1\ 4)(2\ 3)\}$".

Page 183, remark at the bottom of the page. Add the sentence: "A consequence of (a) when $m \geq 1$ is that G has a subgroup of order p; this special case is sometimes called **Cauchy's Theorem in group theory**."

Page 187, line 4 of "Proof of the remainder of Theorem 4.59." Change "orbits of Γ under conjugation by G" to "orbits in Γ under conjugation by G".

Page 192, Example 1 of contravariant functors. In line 6, change "$\mathrm{Hom}_{\mathbb{F}}(V_1, W)$" to "$\mathrm{Hom}_{\mathbb{F}}(V_2, W)$". In line 8, change the right-hand member of the equality from "$F(f)F(g)$" to "$F(f)F(g)(L)$".

Page 192, line −2. Change "$F(f)(\varphi) = f \circ \varphi$" to "$F(f)(\varphi) = \varphi \circ f$".

Page 200, Problem 18, line 2. Change "that is normal in M" to "that is normal in N".

Page 215, line −3. Change "$r^{-1}A^{\mathrm{adj}}$" to "rA^{adj}".

Page 217, line 5 of the paragraph beginning "Let us return." Change "$M_n(A)$" to "$M_n(\mathbb{K})$".

Page 240, Problem 12. Insert after the problem number: "(**Special case of Jordan–Chevalley decomposition**)".

Page 241, Problem 13. Insert after the problem number: "(**Special case of Jordan–Chevalley decomposition**, continued)".

Page 248, line −4. Change "$\langle u, v)$" to "$\langle u, v\rangle$".

Page 262, line 2. Change "$E \in E$" to "$e \in E$".

Page 280, line 10. Change "$\Phi i = \varphi$" to "$\Phi i = j\varphi$".

Page 285, lines −5 and −4. Change "carry the vector space E over to $\mathbb{K}^n$" to "identify the vector space E with $\mathbb{K}^n$".

Page 316, line 12. Change "$(r_1 b_2 r_2)^{-1}$" to "$(r_1 b_2 r_2^{-1})$".

Page 327, last text line before the second displayed equation. Change "$F : G \to C$" to $F : G \to \mathbb{C}$".

Page 331, lines 3–4. Change "$AR(g) = R(xg) = R(gx) = R(g)A$" to "$AR(x) = R(gx) = R(xg) = R(x)A$".

Page 330, line −6. Change "$Ar_1(g)v$" to "$Ar_1(g)v_1$".

Page 330, line −1. Change "A must be 0" to "$A - \lambda I$ must be 0".

Page 332, line 12. Change "for all $v_1, v_2 \in V_1$" to "for all $v_1, v_1' \in V_1$".

Page 333, line −7. Change "x" to "g" in all three places.

Page 334, lines 21–22. Change "In fact, the sum is invariant under r, and if it is nonzero" to
"We argue by contradiction. The sum is invariant under r, and if it is not all of $C(G, \mathbb{C})$".

Page 353, line 9. Change "M" to "N".

Page 353, line 10. Change "M" to "N".

Page 370, line −9. Change "Section VII.5" to "Section VII.4".

Page 371, item (14), line 3. Change "whose multiplication is" to
"whose ring operations are".

Page 375, fourth new paragraph, line 1. Change "M is a left R submodule" to "M is a left R module".

Page 379, third paragraph, line 1. Change "a nonzero" to "an".

Page 380, line after the definition of **field of fractions**. Change "$(\eta, 1)$" to "$(r, 1)$".

Page 380, statement of Proposition 8.6. Change "nonzero integral domain" to "integral domain".

Page 387, line 7. Change "case $m = 0$ being trivial" to
"case $m = 0$ following since r is not a unit".

Page 390, line −14. Change "proof is application" to "proof is an application".

Page 392, line −6. Insert at the end of the paragraph:
"We shall make computations with $c(A)$ as if it were a member of R, in order to keep the notation simple. To be completely rigorous, one should regard $c(A)$ as an orbit of the group $R^\times$ of units in R, using equality to refer to equality of orbits."

Page 395, line 3. Replace this paragraph with the following shorter argument:
"In the second case, $P(X) = P$ has degree 0 and is prime in R. Put $R' = R(P)$ as in Proof #2 of Theorem 8.18. Then $A(X)B(X)$ maps to zero in the integral domain $R'[X]$, and hence $A(X)$ or $B(X)$ is in $P\,R[X]$." □

Page 395, proof of Corollary 8.22, line 2. Change "primitive" to
"primitive; this adjustment makes use of the hypothesis that p does not divide a_N".

Page 397, Proposition 8.24. Insert a remark after the statement of the proposition:
"REMARK. The proof will show that if M can be generated by n elements, then so can the unital R submodule."

Page 399, Remark with Theorem 8.25. Add a sentence at the end:
"Some people use the name "Fundamental Theorem of Finitely Generated Modules" to refer to Corollary 8.29 rather than to Theorem 8.25."

Page 399, proof of Theorem 8.25, line 3. Change "is 0. Define" to
"is 0. We argue as in the proof of Proposition 2.2. Define".

Page 401, line 8. Change "x_1" to "x_1'".

Page 436, line 8. Change "a_1 and a_2 in J" to "a_1 and a_2 in R".

Page 442, Problem 23. Change "an integer" to "a nonzero integer".

Page 455, line 6. Change "$X - X_n$" to "$X - x_n$".

Page 458, statement of Corollary 9.17. Insert a sentence at the end:
"Conversely if $F(r) = F'(r) = 0$, then $(X - r)^2$ divides $F(X)$."

Page 458, proof of Corollary 9.17. Remove the end-of-proof symbol, and insert a paragraph at the end:
"For the converse, let $F(r) = F'(r) = 0$. Proposition 4.28a shows that $F(X) = (X - r)G(X)$. Differentiating this identity by means of Proposition 9.15 gives $F'(X) = G(X) + (X - r)G'(X)$. Substituting r for X yields $0 = F'(r) = G(r) + 0$ and shows that $G(r) = 0$. By Proposition 4.28, $G(X) = (X - r)H(X)$. Hence $F(X) = (X - r)^2 H(X)$." □

Page 468, footnote 2. Insert at the end:
"Computer calculations have shown that 2^{2^N+1} is not prime if $5 \le N \le 32$".

Page 472, line −10. Change "every root of $\mathbb{K}$" to "every element of $\mathbb{K}$".

Page 473, proof of Corollary 9.29. Insert an opening paragraph that says:
"The minimal polynomial of α_j over $\Bbbk(\alpha_1, \ldots, \alpha_{j-1})$ divides the minimal polynomial of α_j over $\Bbbk$. If the second of these polynomials has distinct roots in a splitting field, so does the first. Thus (c) implies (b)."

Page 474, lines 6–7. Change "we obtain the equivalence of (a) and (c)" to
"we see that (a) implies (c)".

Page 475, proof of Theorem 9.34. Change the first word "We" to
"We may assume that $\Bbbk$ is infinite because Corollary 4.27 shows that the multiplicative group of a finite field is cyclic. With $\Bbbk$ infinite, we".

Page 475, proof of Theorem 9.34. Delete the last sentence of the proof.

Page 476, line 17. Change "some choice of c in $\mathbb{K}$ makes" to
"we can choose c in $\mathbb{K}$ different from all the finitely many quotients $(\beta_i - \beta)(\alpha - \alpha_j)^{-1}$. For such a choice of c,".

Page 535, Problem 15. Change "a is in $\mathbb{Q}$ and r is a member of $\mathbb{C}$ but not $\mathbb{Q}$ with $r^p = a$. Prove that" to
"a is a member of $\mathbb{Q}$ such that $X^p - a$ has no root in $\mathbb{Q}$. If r is a member of $\mathbb{C}$ with $r^p = a$, prove that"

Page 567, line −6. Change "$\psi : N \to N''$" to "$\psi : N' \to N''$".

Page 569, line 1. Change "$\Phi \otimes \Phi'$" to "$\Phi \circ \Phi'$".

Page 569, line 6. Change "$\mathbb{R} = \mathbb{Z}$" to "$R = \mathbb{Z}$".

Page 577, third paragraph of proof of Proposition 10.25. Change "E" to "E'" in 12 places.

Page 581, Problem 17, line 1. Change "canonical R isomorphism" to "canonical isomorphism".

Pages 596–598. The proof starting at the bottom of page 596 has a gap in its last paragraph, as was kindly pointed out by Qiu Ruyue. In addition, the order of the proof can be improved. The entire proof is to be replaced with the material listed under "A Long Correction" at the end of these pages.

Page 602, line 3. Change "$A \mapsto \{A\}$" to "$x \mapsto \{x\}$".

Page 602, line 11. Change "U_α" to "A_α", and change "V_β" to "B_β".

Page 605, answer to Problem 16. Replace "n^2" by "$n(n-1)$" in two places.

Page 618, answer to Problem 18. Change "Section 7" to "Section 8".

Page 670, answer to Problem 33, line 7. Change "A" to "B" twice.

Page 676, answer to Problem 15. Change "In (a) and (b), let" to
"For (a) and (b), Lemma 9.45 shows that $X^p - a$ is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(r) : \mathbb{Q}] = p$. Let".

Page 677, answer to Problem 17. Insert a sentence at the end:
"In other words, the only squares in $\mathbb{K}$ that lie in $\Bbbk$ are the obvious ones."

Pages 703–717. The terms Bezout's identity, Euclid's Lemma, stabilizer, Cauchy's Theorem in group theory, and Jordan–Chevalley decomposition, which have all been introduced in this list of corrections, need to be added to the index.

A Long Correction to the Original Edition

Pages 596–598. Replace the proof starting near the bottom of page 596 with the following:

Proof. A nonempty subset E of X will be called *admissible* for purposes of this proof if $f(E) \subseteq E$ and if the least upper bound of each nonempty chain in E, which exists in X by assumption, actually lies in E. By assumption, X is an admissible subset of X. If x is in X, then the intersection of admissible subsets of X containing x is admissible. Let A_x be the intersection of all admissible subsets

of X containing x. This is admissible, and since the set of all y in X with $x \leq y$ is admissible and contains x, it follows that $x \leq y$ for all $y \in A_x$. By hypothesis, X is nonempty. Fix an element a in X, and let $A = A_a$. The main step will be to prove that A is a chain.

To do so, consider the subset C of members x of A with the property that there is a nonempty chain C_x in A containing a and x such that

- $a \leq y \leq x$ for all y in C_x,
- $f(C_x - \{x\}) \subseteq C_x$, and
- the least upper bound of any nonempty subchain of C_x is in C_x.

The element a is in C because we can take $C_a = \{a\}$. If x is in C, so that C_x exists, let us use the bulleted properties to see that

$$A = A_x \cup C_x. \qquad (*)$$

We have $A \supseteq C_x$ by definition; also $A \cap A_x$ is an admissible set containing x and hence containing A, and thus $A \supseteq A_x$. Therefore $A \supseteq A_x \cup C_x$. For the reverse inclusion it is enough to prove that $A_x \cup C_x$ is an admissible subset of X containing a. The element a is in C_x, and thus a is in $A_x \cup C_x$. For the admissibility we have to show that $f(A_x \cup C_x) \subseteq A_x \cup C_x$ and that the least upper bound of any nonempty chain in $A_x \cup C_x$ lies in $A_x \cup C_x$. Since x lies in A_x, $A_x \cup C_x = A_x \cup (C_x - \{x\})$ and $f(A_x \cup C_x) = f(A_x) \cup f(C_x - \{x\}) \subseteq A_x \cup C_x$, the inclusion following from the admissibility of A and the second bulleted property of C_x.

To complete the proof of $(*)$, take a nonempty chain in $A_x \cup C_x$, and let u be its least upper bound in X; it is enough to show that u is in $A_x \cup C_x$. The element u is necessarily in A since A is admissible. Observe that

$$y \leq x \quad \text{and} \quad x \leq z \qquad \text{whenever } y \text{ is in } C_x \text{ and } z \text{ is in } A_x. \qquad (**)$$

If the chain has at least one member in A_x, then $(**)$ implies that $x \leq u$, and hence the set of members of the chain that lie in A_x forms a nonempty chain in A_x with least upper bound u. Since A_x is admissible, u is in A_x. Otherwise the chain has all its members in C_x, and then u is in C_x by the third bulleted property of C_x.

This completes the proof of $(*)$. Let us now prove that if C_x and $C_{x'}$ exist with $x \leq x'$ and $x \neq x'$, then

$$C_x \subseteq C_{x'}. \qquad (***)$$

In fact, application of $(*)$ to x' gives $A = A_{x'} \cup C_{x'}$. Intersecting both sides with C_x shows that $C_x = (C_x \cap A_{x'}) \cup (C_x \cap C_{x'})$. On the right side, the first member is empty by $(**)$, and thus $C_x = C_x \cap C_{x'}$. This proves $(***)$.

Let C be the set of all members x of A for which C_x exists. We have seen that a is in C. If we apply $(*)$ and $(**)$ first to a member x of C and then to a member x' of C, we see that either $x \leq x'$ or $x' \leq x$. That is, C is a chain.

Let us see that $f(C) \subseteq C$. If x is in C, then the set $D = C_x \cup \{f(x)\}$ certainly has a as a member. The second bulleted property of C_x shows that f carries $C_x - \{x\}$ into D, and also f carries x into D. Thus f carries $D - \{f(x)\}$ into D, and D satisfies the second bulleted property of $C_{f(x)}$. If $\{x_\alpha\}$ is a chain in D with least upper bound u, there are two possibilities. Either u is $f(x)$, which is in D by construction, or u is in C, which contains the least upper bound of any nonempty chain in it. Thus u is in D, D satisfies the third bulleted property of $C_{f(x)}$, and $C_{f(x)}$ exists. In other words, $f(x)$ is in C, and $f(C) \subseteq C$.

Finally let us see that the least upper bound u of an arbitrary chain $\{x_\alpha\}$ in C, which exists in X by assumption, is a member of C. If $x_\alpha = u$ for some α, then $C_u = C_{x_\alpha}$ exists, and u is in C. So assume that $x_\alpha \neq u$ for all α. Our candidate for C_u will be $D = (\bigcup_\alpha C_{x_\alpha}) \cup \{u\}$. This certainly contains a. We check that D satisfies the second bulleted property of C_u. For each α, we can find a β with $x_\alpha \leq x_\beta$ and $x_\alpha \neq x_\beta$, since u is the least upper bound of all the x's. Then $(***)$ gives $C_{x_\alpha} \subseteq C_{x_\beta} - \{x_\beta\}$, and $f(C_{x_\alpha}) \subseteq f(C_{x_\beta} - \{x_\beta\}) \subseteq C_{x_\beta} \subseteq D$. Taking the union over α shows that D satisfies the second bulleted property of C_u.

To see that D satisfies the third bulleted property of C_u, let v be the least upper bound in A of a chain $\{y_\beta\}$ in C_u. If $v \neq u$, then v cannot be an upper bound of $\{x_\alpha\}$. So we can choose some x_{α_0} such that $v \leq x_{\alpha_0}$. Each y_β is $\leq v$, and thus each y_β is $\leq x_{\alpha_0}$. Referring to $(*)$, we see that all y_β's lie in $C_{x_{\alpha_0}}$. By the third bulleted property of $C_{x_{\alpha_0}}$, v is in $C_{x_{\alpha_0}}$. Thus v is in D, and D satisfies the third bulleted property of C_u. Consequently the least upper bound u of an arbitrary chain in C lies in C.

In short, C is an admissible set containing a, and it also is a chain. Since A is a minimal admissible set containing a, $C = A$ and also A is a chain. Let u be the least upper bound of A. We have seen that $f(A) \subseteq A$, and thus $f(u) \leq u$. On the other hand, $u \leq f(u)$ by the defining property of f. Therefore $f(u) = u$, and the proof is complete.

9/7/2015