ERRATA

Abstract Algebra, Third Edition

by D. Dummit and R. Foote

(most recently revised on June 18, 2012)

These are errata for the Third Edition of the book. Errata from previous editions have been fixed in this edition so users of this edition do not need to refer to errata files for the Second Edition (on this web site). Individuals using the Second Edition, however, must make corrections from this list as well as those in the Second Edition errata files (except for corrections to text only needed in the Third Edition; for such text no reference to Second Edition page numbers is given below). Some of these corrections have already been incorporated into recent printings of the Third Edition.

```
page vi (2<sup>nd</sup> Edition p. vi)
from: 7.3 Ring Homomorphisms an Quotient Rings
    to: 7.3 Ring Homomorphisms and Quotient Rings
page 2, Proposition 1(1) (2<sup>nd</sup> Edition p. 2, Proposition 1(1))
from: The map f is injective
    to: If A is not empty, the map f is injective
page 4, line -3 (2<sup>nd</sup> Edition p. 5, line 3)
from: a, b \in \mathbb{Z} - \{0\}
   to: a, b \in \mathbb{Z} and b \neq 0
page 31, The group S_3 table
  last line missing
  add: \sigma_6(1) = 3, \sigma_6(2) = 1, \sigma_6(3) = 2
                                          (1\ 3\ 2)
page 33, Exercise 10, line 2 (2<sup>nd</sup> Edition p. 33, Exercise 10)
from: its least residue mod m when k+i > m
    to: its least positive residue mod m
page 34, line 1 of Definition (2<sup>nd</sup> Edition p. 34, line 1 of Definition)
from: two binary operations
    to: two commutative binary operations
page 39, Example 2, line -4
from: ba = ab^{-1}
   to: ba = a^{-1}b
page 45, Exercise 22 (2<sup>nd</sup> Edition p. 46, Exercise 22)
from: is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4
    to: is isomorphic to S_4
page 51, line -1 (2<sup>nd</sup> Edition p. 52, line -1)
from: see Exercise 1 in Section 1.7
   to: see Exercise 4(b) in Section 1.7
```

```
page 65, line 2 of Exercise 16(c) (2<sup>nd</sup> Edition p. 66, Exercise 16(c))
 from: if and only H
    to: if and only if H
page 71, Exercise 5 (2<sup>nd</sup> Edition p. 72, Exercise 5)
 from: there are 16 such elements x
    to: there are 8 such elements x
page 84, line 11 of Example 2 (2<sup>nd</sup> Edition p. 85, line 11 of Example 2)
from: By Proposition 2.6
    to: By Theorem 2.7(1)
page 84, line -6 of Example 2 (2<sup>nd</sup> Edition p. 85, line -6 of Example 2)
 from: By Proposition 2.5
    to: By Theorem 2.7(3)
page 86, Exercise 14(d) (2<sup>nd</sup> Edition p. 87, Exercise 14(d))
 from: root
    to: roots
page 98, Figure 6
  add: hatch marks to upper right and lower left lines of the central diamond (to indicate AB/B \cong
       A/A \cap B).
page 103, line 3 of Definition (2<sup>nd</sup> Edition p. 104, line 3 of Definition)
 from: N_{i+1}/N_i a simple group
    to: N_{i+1}/N_i is a simple group
page 114, line 3 in proof of Proposition 2 (2<sup>nd</sup> Edition p. 116, line 3 of proof)
 from: b \in G
    to: g \in G
page 128, second line above last display (2<sup>nd</sup> Edition p. 130, line -3)
 from: any element of odd order
    to: any nonidentity element of odd order
page 132, Exercise 33, line -1 (2<sup>nd</sup> Edition p. 134, line -1 of Exercise 33)
 from: See Exercises 6 and 7 in Section 1.3
    to: See Exercises 16 and 17 in Section 1.3
page 132, Exercise 36(c) (2<sup>nd</sup> Edition p. 135, Exercise 36(c))
 from: q and h lie in the center of G
    to: g and h lie in the center of G and g = h^{-1}
page 139, Definition (1) (2<sup>nd</sup> Edition p. 141, Definition (1))
 from: A group of order p^{\alpha} for some \alpha \geq 1
    to: A group of order p^{\alpha} for some \alpha \geq 0
```

```
page 143, last line of first Example (2<sup>nd</sup> Edition p. 145, line -2)
 from: Theorem 17
    to: Proposition 17
page 145, line -7 (2<sup>nd</sup> Edition p. 148, line 5)
 from: less that
    to: less than
page 148, Exercise 47(i) (2<sup>nd</sup> Edition p. 151, Exercise 47(i))
from: that has some prime divisor p such that n_p is not forced to be 1
    to: for each prime divisor p of n the corresponding n_p is not forced to be 1
page 149, Exercise 54, line 4 (2<sup>nd</sup> Edition p. 151, line 4 of Exercise 54)
 from: G/N acts as automorphisms of N
    to: G/C_G(N) acts as automorphisms of N
page 151, Exercise 6, line -2 (2<sup>nd</sup> Edition p. 153, line -2 of Exercise 6)
 from: every pair of elements of D lie in a finite simple subgroup of D
    to: every pair of elements of A lie in a finite simple subgroup of A
page 158, line 3 after the Definition (2<sup>nd</sup> Edition p. 160)
 from: n-tuple
    to: r-tuple
page 174, Exercise 18 (2<sup>nd</sup> Edition p. 176, Exercise 18)
 from: Let K_1, K_2, \ldots, K_n be etc.
    to: Let G_1, G_2, \ldots, G_n be etc. (change K_i to G_i throughout the exercise).
page 187, Exercise 23, line 4 (2<sup>nd</sup> Edition p. 189, line 4 of Exercise 23)
 from: from G into
    to: from K into
page 191, Proposition 2 (2<sup>nd</sup> Edition p. 193, Proposition 2)
 from: nilpotence class at most a-1.
    to: nilpotence class at most a-1 for a \ge 2 (and class equal to a when a=0 or 1).
page 191, line 3 of the proof of Proposition 2 (2<sup>nd</sup> Edition p. 193)
 from: Thus if Z_i(P) \neq G
    to: Thus if Z_i(P) \neq P
page 194, Theorem 8, line 4 (2<sup>nd</sup> Edition p. 196, Theorem 8, line 4)
from: Z_i(G) \le G^{c-i-1} \le Z_{i+1}(G) for all i \in \{0, 1, ..., c-1\}.
    to: G^{c-i} \leq Z_i(G) for all i \in \{0, 1, ..., c\}.
page 198, Exercise 18 (2<sup>nd</sup> Edition p. 200, Exercise 18)
 from: then G'' = 1
    to: then G'' = G'''
page 199, Exercise 22 (2<sup>nd</sup> Edition p. 201, Exercise 22)
 from: Prove that
    to: When G is a finite group prove that
```

```
page 201, line 2 of Exercise 38 (2<sup>nd</sup> Edition p. 203, Exercise 38)
 from: The group G/M
    to: The group P/M
page 209, Proposition 14(1)
 from: n_3 = 7
    to: n_3 = 28
page 216, line 4 after displayed steps (1) and (2) (2<sup>nd</sup> Edition p. 217, line -3)
 from: are equal if and only if n=m and \delta_i=\epsilon_i, 1\leq i\leq n
    to: are equal if and only if n = m, r_i = s_i and \delta_i = \epsilon_i, 1 \le i \le n
page 217, line 2 after first display (2<sup>nd</sup> Edition p. 218, line 2 after second display)
 from: A(F) be the subgroup
    to: A(S) be the subgroup
page 255, line 2 of Example 1 (2<sup>nd</sup> Edition p. 256, line 2 of Example 1)
 from: We saw in Section 3
    to: We saw in Section 1
page 260, Exercise 40(iii) (2<sup>nd</sup> Edition p. 261, Exercise 40(iii))
 from: R/\eta(R)
    to: R/\mathfrak{N}(R)
page 263, line 2 of the Definition (2<sup>nd</sup> Edition p. 264)
 from: ring of fractions of D with respect to R
    to: ring of fractions of R with respect to D
page 269, line 2 of Exercise 10(c) (2<sup>nd</sup> Edition p. 270, Exercise 10(c))
 from: then A may likewise
    to: then P may likewise
page 269, line 2 of Exercise 11(d) (2<sup>nd</sup> Edition p. 270, Exercise 11(d))
 from: Prove that every ideal of
    to: Prove that every nonzero ideal of
page 269, lines 1 and 2 of Exercise 11(e) (2<sup>nd</sup> Edition p. 270, Exercise 11(e))
 from: in the direct limit \mathbb{Z}_p satisfying a_i^p
    to: in the inverse limit \mathbb{Z}_p satisfying a_i^{p-1}
page 282, second display (2<sup>nd</sup> Edition p. 283, second display) from: 0 < N(\frac{\alpha}{\beta}s - t) = \frac{(ay - 19bx - cq)^2 + 19(ax + by + cz)^2}{c^2} \le \frac{1}{4} + \frac{19}{c^2}
        and so (*) is satisfied with this s and t provided c \geq 5.
    to: 0 < N(\frac{\alpha}{\beta}s - t) = \frac{(ay - 19bx - cq)^2 + 19(ax + by + cz)^2}{c^2} = \frac{r^2 + 19}{c^2} \le \frac{1}{4} + \frac{19}{c^2}
        and so (*) is satisfied with this s and t provided c \ge 5 (note r^2 + 19 \le 23 when c = 5).
page 283, Exercise 8 (2<sup>nd</sup> Edition p. 284, Exercise 8)
```

from: D is a multiplicatively closed subset of R

to: D is a multiplicatively closed subset of R with $0 \notin D$

page 290, line 5 (2nd Edition p. 291, line 5)

from: is irreducible in $\mathbb{Z}[i]$ to: is irreducible in \mathcal{O}

page 292, line 4 of Example

```
from: (4+i)(5-2i) = 22-3i, (4-i)(5-2i) = 22+3i
to: (4+i)(5-2i) = 22-3i, (4-i)(5+2i) = 22+3i
```

page 304, line 13 (2nd Edition p. 305, line 3)

from: one fewer irreducible factors to: one fewer irreducible factor

page 306, line 3 (2nd Edition p. 307, line3)

from: where p'(x) is irreducible in both R[x] and F[x].

to: where p'(x) is irreducible in R[x] if and only if it is irreducible in F[x].

page 312, Exercise 16(b) (2nd Edition p. 313, Exercise 16(b))

from: Prove that f

to: If $f(0) \neq 0$, prove that f

page 316, line -6

from: Suppose next that d < N. In this case $a \in L_d$ for some d < N, to: Thus $a \in L_d$ for some d < N,

page 316, line -5

```
from: \cdots + r_{n_d}b_{n_d} for some \cdots + r_{n_d}f_{n_d} is a to: \cdots + r_{n_d}b_{d,n_d} for some \cdots + r_{n_d}f_{d,n_d} is a
```

page 318, line 7 after the Definition

```
from: L(fg) = L(f) + L(g)
to: L(fg) = L(f)L(g)
```

page 323, line -6

from: among the differences $S(g_i, g_j)$

to: among the remainders of the differences $S(g_i, g_j)$

page 330, line 7

Replace from "We close this section ..." to "Example" with:

We close this section by showing how to compute the basic set-theoretic operations of sums, products and intersections of ideals in polynomial rings. Suppose $I=(f_1,\ldots,f_m)$ and $J=(h_1,\ldots,h_k)$ are two ideals in $F[x_1,\ldots,x_n]$. Then $I+J=(f_1,\ldots,f_m,h_1,\ldots,h_k)$ and $IJ=(f_1h_1,\ldots,f_ih_j,\ldots,f_mh_k)$. The following proposition shows how to compute the intersection of any two ideals.

Proposition 30. Suppose $I=(f_1,\ldots,f_m)$ and $J=(h_1,\ldots,h_k)$ are two ideals in $F[x_1,\ldots,x_n]$. If \mathcal{I} denotes the ideal generated by $tf_1,\ldots,tf_m,(1-t)h_1,\ldots,(1-t)h_k$ in $F[t,x_1,\ldots,x_n]$, then $I\cap J=\mathcal{I}\cap F[x_1,\ldots,x_n]$. In particular, $I\cap J$ is the first elimination ideal of \mathcal{I} with respect to the ordering $t>x_1>\cdots>x_n$.

Proof: If $f \in I \cap J$, then f = tf + (1-t)f, and noting both tf and (1-t)f are in \mathcal{I} shows $I \cap J \subseteq \mathcal{I} \cap F[x_1, \dots, x_n]$. Conversely, suppose $f \in \mathcal{I} \cap F[x_1, \dots, x_n]$. Then $f = f(x_1, \dots, x_n)$.

 $a_1tf_1+\cdots+a_mtf_m+b_1(1-t)h_1+\cdots+b_k(1-t)h_k$ for some polynomials $a_1,\ldots,a_m,b_1,\ldots,b_k$ in $F[t,x_1,\ldots,x_n]$. Setting t=0 (which does not alter f) shows f is an $F[x_1,\ldots,x_n]$ -linear combination of h_1,\ldots,h_k , so $f\in J$. Similarly, setting t=1 shows $f\in I$, so $f\in I\cap J$. Finally, since $I\cap J=\mathcal{I}\cap F[x_1,\ldots,x_n],\ I\cap J$ is the first elimination ideal of \mathcal{I} with respect to the ordering $t>x_1>\cdots>x_n$.

By Propositions 29 and 30, if $I=(f_1,\ldots,f_m)$ and $J=(h_1,\ldots,h_k)$, then the elements not involving t in a Gröbner basis for the ideal generated by tf_1,\ldots,tf_m and $(1-t)h_1,\ldots,(1-t)h_k$ in $F[t,x_1,\ldots,x_n]$, computed for the lexicographic monomial ordering $t>x_1>\cdots>x_n$, give a Gröbner basis for the ideal $I\cap J$ in $F[x_1,\ldots,x_n]$.

page 331, Exercise 3(i)

from: minimum element to: minimal element

page 332, Exercise 9(b)

from: grlex order to: grevlex order

page 332, Exercise 15(a)

from: Prove that $\{g_1, \ldots, g_m\}$ is a minimal Gröbner basis for the ideal I in R if to: Prove that the subset $\{g_1, \ldots, g_m\}$ of the ideal I in R is a minimal Gröbner basis of I if

page 332, Exercise 16, line 3

from: $(LT(g_1), \ldots, LT(g_m), LT(S(g_i, g_j))$ is strictly larger than the ideal $(LT(g_1), \ldots, LT(g_m))$. Conclude that the algorithm ...

to: $(LT(g_1), \ldots, LT(g_m), LT(r))$ is strictly larger than the ideal $(LT(g_1), \ldots, LT(g_m))$, where $S(g_i, g_j) \equiv r \mod G$. Deduce that the algorithm ...

page 333, display in Definition following Exercise 33

from: $rJ \in I$ to: $rJ \subseteq I$

page 334, Exercise 43(a)

from: Use Exercise 30 to: Use Exercise 39

page 334, Exercise 43(b)

from: Use Exercise 33(a) to: Use Exercise 42(a)

page 334, line 3 of Exercise 43(c)

from: ideal defined in Exercise 32, to: ideal quotient (cf. Exercise 41),

page 348, line 6 (2nd Edition p. 329, line 6)

from: When R is a field, however

to: When R is a field and $M \neq 0$, however

```
page 350, line 2 of Exercise 4 (2<sup>nd</sup> Edition p. 331, Exercise 4)
from: \varphi(\overline{k}) = ka
    to: \varphi_a(\overline{k}) = ka
page 357, Exercise 21(i) (2<sup>nd</sup> Edition p. 338, Exercise 21(i))
    replace (i) with: the map from the (external) direct sum \bigoplus_{i \in I} N_i to the submodule of M
    generated by all the N_i's by sending a tuple to the sum of its components is an isomorphism
    (cf. Exercise 20)
page 360, line 6 of second paragraph (2^{nd} Edition p. 340, line -5)
    Remove the second comma in: i.e., ,
page 370, line 16 of Example 8 (2<sup>nd</sup> Edition p. 351, line 4)
from: f(n \mod I)
    to: f(n \mod IN)
page 372, Corollary 16(2), top line of commutative diagram
from: M \times \cdots \times M_n \xrightarrow{\iota} M \otimes \cdots \otimes M_n
to: M_1 \times \cdots \times M_n \xrightarrow{\iota} M_1 \otimes \cdots \otimes M_n
page 374, line 2 of second Remark (2<sup>nd</sup> Edition p. 355 line 2)
 from: Section 11.6
    to: Section 11.5
page 375, line 4 of Exercise 8 (2nd Edition p. 356, Exercise 8)
 from: relation (u, n) \sim (u', n) if and only if u'n = un' in N.
    to: relation (u,n) \sim (u',n') if and only if xu'n = xun' in N for some x \in U.
page 377, Exercise 23 (2<sup>nd</sup> Edition p. 357, Exercise 23)
 from: Proposition 19
    to: Proposition 21
page 385, title of subsection following Proposition 26
 from: Modules and \operatorname{Hom}_{R}(D, \underline{\hspace{1cm}})
    to: Projective Modules and \operatorname{Hom}_{R}(D, \underline{\hspace{1cm}})
page 395, line 7 after the Definition (2<sup>nd</sup> Edition p. 376, line 4)
 from: Put another way, the map \operatorname{Hom}_R(D, )
    to: Put another way, the map Hom_R(\cdot, D)
page 396, line -2 above Proposition 36 (2<sup>nd</sup> Edition p. 376)
 from: Exercises 18 and 19
    to: Exercises 19 and 20
page 398, proof of Theorem 38 (2<sup>nd</sup> Edition p. 378)
 from: Exercises 15 to 17
    to: Exercises 15 and 16
page 399, line 8 (2<sup>nd</sup> Edition p. 379, line 22)
 from: The map 1 \otimes \varphi is not in general injective
```

to: The map $1 \otimes \psi$ is not in general injective

page 401, line 2 of Example 1 (2nd Edition p. 381, line 2 of Example 1)

from: $\mathbb{Z}/2\mathbb{Z}$ not a flat module to: $\mathbb{Z}/2\mathbb{Z}$ is not a flat module

page 403, Exercise 1(d) (2nd Edition p. 383, Exercise 1(d))

from: if β is injective, α and γ are surjective, then γ is injective to: if β is injective, α and φ are surjective, then γ is injective

page 405, Exercise 15 (2nd Edition p. 385, Exercise 115)

change exercise to:

Let M be a left \mathbb{Z} -module and let R be a ring with 1.

- (a) Show that $\operatorname{Hom}_{\mathbb{Z}}(R,M)$ is a left R-module under the action $(r\varphi)(r') = \varphi(r'r)$ (see Exercise 10).
- (b) Suppose that $0 \to A \xrightarrow{\psi} B$ is an exact sequence of R-modules. Prove that if every \mathbb{Z} -module homomorphism f from A to M lifts to a \mathbb{Z} -module homomorphism F from B to M with $f = F \circ \psi$, then every R-module homomorphism f' from A to $\operatorname{Hom}_{\mathbb{Z}}(R,M)$ lifts to an R-module homomorphism F' from B to $\operatorname{Hom}_{\mathbb{Z}}(R,M)$ with $f' = F' \circ \psi$. [Given f', show that $f(a) = f'(a)(1_R)$ defines a \mathbb{Z} -module homomorphism of A to M. If F is the associated lift of f to G, show that G'(a) = F(f) defines an G-module homomorphism from G to G to G that lifts G that G is an G-module homomorphism from G to G that G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G to G that G is an G-module homomorphism from G is an G-module homomorphism from G-module homomorphism G-module homomo
- (c) Prove that if Q is an injective \mathbb{Z} -module then $\operatorname{Hom}_{\mathbb{Z}}(R,Q)$ is an injective R-module.

page 407, last line of Exercise 27(a) (2nd Edition p. 387, Exercise 27(a))

from: where π_1 and π_2 are the natural projections onto

to: where π_1 and π_2 are the restrictions to X of the natural projections from $A \oplus B$ onto

page 409, line 2 of Definition (1) (2nd Edition p. 389, Definition (1))

from: and $v_1, v_2, \ldots, v_n \in S$ to: and v_1, v_2, \ldots, v_n distinct elements of S

page 423, line 3 of Exercise 9 (2nd Edition p. 403, Exercise 9)

from: If $\varphi|_W$ and $\widetilde{\varphi}$ are to: If $\varphi|_W$ and $\overline{\varphi}$ are

page 426, line 2 of Exercise 21(b) (2nd Edition p. 406, Exercise 21(b))

from: 6zto: +6z

page 433, proof of Theorem 19, line 3

from: $= E_v(f) + \alpha E_g(v)$ to: $= E_v(f) + \alpha E_v(g)$

page 435, Exercise 1

change exercise to:

Let V be a vector space over F of dimension $n < \infty$. Prove that the map $\varphi \mapsto \varphi^*$ in Theorem 20 is a vector space isomorphism of $\operatorname{End}(V)$ with $\operatorname{End}(V^*)$, but is not a ring homomorphism when n > 1. Exhibit an F-algebra isomorphism from $\operatorname{End}(V)$ to $\operatorname{End}(V^*)$.

```
page 442, line -8 (2<sup>nd</sup> Edition p. 422, line -8)
 from: \varphi: M \to A is an R-algebra
    to: \varphi: M \to A is an R-module
page 445, second display in Theorem 34(2) (2<sup>nd</sup> Edition p. 425, Theorem 34(2))
 from: \iota(m_1,\ldots,m_k)=m_1\otimes\cdots\otimes m_n \bmod \mathcal{C}(M)
    to: \iota(m_1,\ldots,m_k)=m_1\otimes\cdots\otimes m_k \bmod \mathcal{C}^k(M)
page 459, line -8 (2<sup>nd</sup> Edition p. 439,line -8)
 from: y_i = a_{1i}e_i + a_{2i}e_2 + \dots + a_{ni}e_i
    to: y_i = a_{1i}e_1 + a_{2i}e_2 + \cdots + a_{ni}e_n
page 468, Exercise 1(a) (2<sup>nd</sup> Edition p. 448, Exercise 1(a))
 from: Change first two sentences to
    to: Show that any finite number of elements of M, one of which is torsion, are R-linearly
        dependent.
page 469, line 1 of Exercise 10 (2<sup>nd</sup> Edition p. 449, Exercise 10)
 from: N an R-module
    to: N a torsion R-module
page 479, last sentence of second paragraph (2<sup>nd</sup> Edition p. 459, second paragraph)
 from: the degree of the minimal polynomial for A has degree at most n
    to: the minimal polynomial for A has degree at most n
page 510, line 1 of text (2<sup>nd</sup> Edition p. 490, line 1 of text)
 from: F is a commutative ring with
    to: F is a nonzero commutative ring with
page 516, line 3 or Remark (2<sup>nd</sup> Edition p. 496, line 3 of Remark)
 from: examples indicates
    to: examples indicate
page 526, lines 1 and 2 (2<sup>nd</sup> Edition p. 505, last paragraph lines 1 and 2)
 from: the algebraic \alpha is obtained by adjoining the element \alpha to F
    to: the algebraic element \alpha is obtained by adjoining \alpha to F
page 555, Exercise 7, bounds for product (2<sup>nd</sup> Edition p. 535, Exercise 7)
 from: d \mid n
    to: d \mid m
page 566, Example 7, first line after second display
 from: we see that \sigma_p^{p^n} = 1
to: we see that \sigma_p^n = 1
page 579, line -11 (2<sup>nd</sup> Edition p. 559, line -11)
 from: minimal polynomial \Phi_4(x)
    to: minimal polynomial \Phi_8(x)
```

page 582, Exercise 17 (2nd Edition p. 563, Exercise 17)

from: Let K/F be any finite extension

to: Let K/F be any finite separable extension

page 584, Exercise 24 (2nd Edition p. 564, Exercise 24)

change exercise to:

Prove that the rational solutions $a,b\in\mathbb{Q}$ of Pythagoras' equation $a^2+b^2=1$ are of the form $a=\frac{s^2-t^2}{s^2+t^2}$ and $b=\frac{2st}{s^2+t^2}$ for some $s,t\in\mathbb{Q}$. Deduce that any right triangle with integer sides has sides of lengths $((m^2-n^2)d,\,2mnd,\,(m^2+n^2)d)$ for some integers m,n,d. [Note that $a^2+b^2=1$ is equivalent to $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib)=1$, then use Hilbert's Theorem 90 above with $\beta=s+it$.]

page 585, Exercise 29(b) (2nd Edition p. 565, Exercise 29(b))

from: Prove that the element t =

to: Prove that the element s =

page 585, Exercise 29(c) (2nd Edition p. 565, Exercise 29(c))

from: Prove that k(t)

to: Prove that k(s)

page 597, line 1 of Example 2

from: $\mathbb{Q}(\zeta_{13})$, For p to: For p

page 617, Exercises (2nd Edition p. 598, Exercises)

The first 10 exercises, excluding Exercise 3, are over the field \mathbb{Q} .

page 638, Exercise 18 (2nd Edition p. 619, Exercise 18)

from: Let $D \in \mathbb{Z}$ be a squarefree integer to: Let $D \neq 1$ be a squarefree integer

page 654, Exercise 16 (2nd Edition p. 635, Exercise 16)

from: Prove that F does not contain all quadratic extensions of \mathbb{Q} .

to: Prove that F does contain all quadratic extensions of \mathbb{Q} . [One way is to consider the polynomials $x^3 + 3ax + 2a$ for $a \in \mathbb{Z}^+$.]

page 670, line 2 of Exercise 34 (2nd Edition p. 648, Exercise 34)

from: $\operatorname{Ass}_R(N) \subseteq \operatorname{Ass}_R(M)$ to: $\operatorname{Ass}_R(L) \subseteq \operatorname{Ass}_R(M)$

page 679, line 12

from: $\mathbb{R}[x, y, z, t]$ to: $\mathbb{R}[x, y, t]$

page 687, Exercise 13 (2nd Edition p. 662, Exercise 13)

change exercise to:

Let V be a nonempty affine algebraic set. Prove that if k[V] is the direct sum of two nonzero ideals then V is not connected in the Zariski topology. Prove the converse if k is

algebraically closed. [Use Theorem 31.] Give a counterexample to the converse when k is not algebraically closed.

```
page 707, line 2 of Corollary 37(1) (2<sup>nd</sup> Edition p. 678, Corollary 29(1))
 from: if and only if D contains no zero divisors of R
    to: if and only if D contains no zero divisors or zero
page 713, line 7 of Example 1
 from: P_2 \cap \mathbb{Q}[y, z] = (y^5 - z^4)
to: P_2 = P \cap \mathbb{Q}[y, z] = (y^5 - z^4)
page 721, line 4 after commutative diagram (2<sup>nd</sup> Edition p. 688, line 2)
                                       [2<sup>nd</sup> Edition: By Proposition 30(1)]
 from: By Proposition 38(1)
                                       [2<sup>nd</sup> Edition: By Proposition 36(1)]
    to: By Proposition 46(1)
page 728, Exercise 21, line 1
 from: Suppose \varphi: R \to S is a ring homomorphism
    to: Suppose \varphi: R \to S is a ring homomorphism with \varphi(1_R) = 1_S
page 754, line 2 of Exercise 8 (2<sup>nd</sup> Edition p. 720, Exercise 8)
 from: Observe the
    to: Observe that
page 756, line 1 of proof of Proposition 5 (2<sup>nd</sup> Edition p. 722, proof of Proposition 5)
 from: \nu(u) + \nu(v) = \nu(uv) = 1
    to: \nu(u) + \nu(v) = \nu(uv) = \nu(1) = 0
page 761, line 3 of proof of Proposition 10 (2<sup>nd</sup> Edition pp. 727)
 from: g: A \to F by f(c) =
    to: g: A \to F by g(c) =
page 764, line -2 (2<sup>nd</sup> Edition p. 730, line -2)
 from: Every Principal Ideal Domain is
    to: Every Principal Ideal Domain that is not a field is
page 767, line 5 (2^{nd} Edition pp. 733)
 from: complete
    to: completes
page 774, line 2 of Exercise 12
 from: in R are relatively prime
    to: in R that are relatively prime
page 775, lines 1 to 3 of Exercise 24(d) (2<sup>nd</sup> Edition pp. 741-2, Exercise 24(d))
from: P_3 = (3, 1 + \sqrt{-5}) = (3, 5 - \sqrt{-5}) \dots [Check that \sqrt{-10} = -(5 - \sqrt{-5})\omega/3.]

to: P_3 = (3, 1 - \sqrt{-5}) = (3, 5 + \sqrt{-5}) \dots [Check that \sqrt{-10} = (5 + \sqrt{-5})\omega/3.]
page 781, bottom row of diagram (17.9) (2<sup>nd</sup> Edition p. 748, diagram (17.9))
 from: 0 \longrightarrow \operatorname{Hom}_R(A, D) \longrightarrow
```

to: $0 \longrightarrow \operatorname{Hom}_R(A', D) \longrightarrow$

```
page 793, line 4 of Exercise 11(c) (2<sup>nd</sup> Edition p. 760, Exercise 11(c))
 from: projection maps I \to I_i
    to: projection maps I \to I/I_i
page 794, Exercise 17 (2<sup>nd</sup> Edition p. 761, Exercise 17)
 from: for any abelian group A
    to: for any abelian group B
page 799, line 2 after (17.17) (2<sup>nd</sup> Edition p. 765, line 2 after (17.17))
 from: in Theorem 8
    to: in Theorem 10
page 800, line -7 (2<sup>nd</sup> Edition p. 766, line -7)
 from: H^n(G,A) \cong Ext^n(\mathbb{Z},A)
    to: H^n(G,A) \cong Ext^n_{\mathbb{Z}G}(\mathbb{Z},A)
page 801, line 4 (2<sup>nd</sup> Edition p. 767, line 4)
 from: 1 if n is odd
    to: a if n is odd
page 812, Exercise 18(a) (2<sup>nd</sup> Edition p. 778, Exercise 18(a))
 from: from \mathbb{Z}/(m/d)\mathbb{Z} to \mathbb{Z}/m\mathbb{Z} if n is odd, and from 0 to 0 if n is even, n \geq 2,
    to: from 0 to 0 if n is odd, and from \mathbb{Z}/(m/d)\mathbb{Z} to \mathbb{Z}/m\mathbb{Z} if n is even, n \ge 2,
page 813, line 3 of Exercise 19 (2<sup>nd</sup> Edition p. 779, Exercise 19)
 from: p-primary component of H^1(G,A)
    to: p-primary component of H^n(G,A)
page 815, line 2 of Proposition 30 (2<sup>nd</sup> Edition p. 781)
 from: group homomorphisms from G to H
    to: group homomorphisms from G to A
page 816, line -13 (2<sup>nd</sup> Edition p. 782, line -13)
 from: bijection between the elements of
    to: bijection between the cyclic subgroups of order dividing n of
page 823, Exercise 9(b) (2<sup>nd</sup> Edition p. 789, Exercise 9(b))
 from: H^1(A_n, V) = 0 for all p
   to: |H^1(A_n, V)| = \begin{cases} 3, & \text{if } p = 3 \text{ with } n = 4 \text{ or } 5 \\ 0, & \text{otherwise} \end{cases}
page 832, lines -10 and -14 (2<sup>nd</sup> Edition p. 798, lines -6 and -10)
 from: L
    to: K
page 853, line 4 of Exercise 17 (2<sup>nd</sup> Edition p. 819, Exercise 17)
 from: Your proof ...
    to: Your proof that \varphi has degree 1 should also work for infinite abelian groups when \varphi has
        finite degree.
```

page 869, line -6 (2nd Edition p. 835, line -6)

from: the isotypic components of G to: the isotypic components of M

page 885, Exercise 8 (2nd Edition p. 851, Exercise 8)

from: This table contains nonreal entries.

to: This table contains irrational entries.

page 893, line 4 (2nd Edition p. 859, line 4)

from: a proper, nontrivial subgroup of G

to: a proper, nontrivial normal subgroup of G

page 897, line 7(2nd Edition p. 863)

Replace from "Let $\psi \dots$ " to end of proof with:

Let \mathcal{C} be the set of nonprincipal irreducible characters of Q. For each $\psi \in \mathcal{C}$ and each $i = 0, 1, \ldots, p-1$ define

$$\psi_i(h) = \psi(x^i h x^{-i})$$
 for all $h \in Q$.

Since ψ_i is a homomorphism from Q into \mathbb{C}^{\times} it is also an irreducible character of Q. Thus $P = \langle x \rangle$ permutes \mathcal{C} via the (right) action $\psi^{x^i} = \psi_i$ (see Exercise 10).

If $\psi_i = \psi_j$ for some i > j then $\psi(x^i h x^{-i}) = \psi(x^j h x^{-j})$ and so $\psi(h) = \psi(x^{i-j} h x^{j-i})$ for all $h \in Q$. Let k = i - j so that $\psi = \psi_k$. Thus $\ker \psi = \ker \psi_k$ and it follows that x^k normalizes $\ker \psi$. Since $\langle x \rangle = \langle x^k \rangle$ acts irreducibly on Q, $\ker \psi = 1$. Thus ψ is a faithful character. But G is a Frobenius group so $h \neq x^k h x^{-k}$ for every nonidentity $h \in Q$, contrary to $\psi(h) = \psi(x^k h x^{-k})$. This proves $\psi_0, \ldots, \psi_{p-1}$ are distinct irreducible characters of Q, i.e., P acts without fixed points on C.

Next let $\psi \in \mathcal{C}$ and let $\Psi = \operatorname{Ind}_Q^G(\psi)$. We use the orthogonality relations and the preceding results to show that Ψ is irreducible. Since $1, x^{-1}, \dots, x^{-(p-1)}$ are coset representatives for Q in G and, by Corollary 12, Ψ is zero on G - Q we have

$$||\Psi||^{2} = \frac{1}{|G|} \sum_{h \in Q} \Psi(h) \overline{\Psi(h)}$$

$$= \frac{1}{|G|} \sum_{h \in Q} \sum_{i=0}^{p-1} \psi(x^{i} h x^{-i}) \sum_{j=0}^{p-1} \overline{\psi(x^{j} h x^{-j})}$$

$$= \frac{1}{|G|} \sum_{i,j=0}^{p-1} \sum_{h \in Q} \psi_{i}(h) \overline{\psi_{j}(h)}$$

$$= \frac{1}{|G|} |Q| \sum_{i,j=0}^{p-1} (\psi_{i}, \psi_{j})_{Q} = \frac{1}{|G|} |Q|_{p} = 1$$

where the second line follows from the definition of the induced character Ψ , and the last line follows because the previous paragraph gives $(\psi_i, \psi_j)_Q = \delta_{ij}$. This proves Ψ is an irreducible character of G.

Finally we show that every irreducible character of G of degree > 1 is induced from some nonprincipal degree 1 character of Q by counting the number of distinct irreducible characters of G obtained this way. By parts (1) and (2) the number of irreducible characters

of G (= the number of conjugacy classes) is $p + (q^a - 1)/p$ and the number of degree 1 characters is p. Thus the number of irreducible characters of G of degree > 1 is $(q^a - 1)/p$. Each $\psi \in \mathcal{C}$ induces to an irreducible character of degree p of G. Characters ψ_i, ψ_j in the same orbit of P acting on \mathcal{C} induce to the same character of G (which is zero outside Q and on Q it is $\sum_{i=0}^{p-1} \psi_i$). One easily computes that characters in different orbits of P on \mathcal{C} induce to orthogonal irreducible characters of G. Since P acts without fixed points on \mathcal{C} , the number of its orbits is $|\mathcal{C}|/p = (q^a - 1)/p$. This accounts for all irreducible characters of G of degree > 1, and all such have degree p. The proof is complete.

```
page 899, line 1 of item (3) (2<sup>nd</sup> Edition p. 865)

from: let Q_3 be a Sylow 11-subgroup of G

to: let Q_3 be a Sylow 13-subgroup of G

page 907, Exercise 1(a) (2<sup>nd</sup> Edition p. 873, Exercise 1(a))

from: a 3-tuple in A \times A \times A maps to an ordered pair in A \times A

to: an ordered pair in A \times A maps to a 3-tuple in A \times A \times A

page 912, line 6 (2<sup>nd</sup> Edition p. 878, line 6)

from: if A \neq B or C \neq D

to: if A \neq C or B \neq D
```