

ERRATA for “A First Course in Abstract Algebra,” 2nd Ed., J. Rotman

July 7, 2003

I thank everyone, especially, Dan Anderson, Carl Jockusch, and David Leep, who has pointed out errors to me. If you have found any errors not listed below, please send them to me at

rotman@math.uiuc.edu

Page 5: Replace line 12 by the following.

is not divisible by 2, 3, 5, . . . , or 31, then it is prime. There are 11 such

Page 17 last line

the last term in the sum should be $1x^4$ (and not $1x^5$).

Page 20: Remove the first three lines of the proof of Lemma 1.15, and rewrite the fourth line, after removing *Inductive Step*:

We must show, for all $n \geq 1$, that if

Page 28: the power of -1 in the power series for $\sin x$ should be $(-1)^n$ instead of $(-1)^{n-1}$; that is,

$$\cdots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} + \cdots .$$

Page 31: line 2; fix the exponent on e , so it reads

$$e^{2\pi ik/n} \sqrt[n]{a}$$

Page 35: line 13; change $D_0 f(x)$ to $D^0 f(x)$.

Page 35: line -1 ; change $|z^2|$ to $z\bar{z}$.

Page 38: line 4 of the pseudocode should read: WHILE $r \geq a$ DO

Page 38: line 5 of the pseudocode should read: $r := r - a$

Page 47: lines 18 and 19 should read:

and $a = r_1$. Repeated application of the division algorithm gives integers q_i , positive integers r_i , and equations:

Page 53: line -1 ; should read $7^2 = 49$;

Page 56: the parenthetical phrase in Exercise 1.45(i) should read:

Find the gcd $d = (12327, 2409)$ (i.e., $n > 1$ and n is not divisible by the square of any prime)

Page 56: Rewrite Exercise 1.47 as follows:

Find $\gcd d = (7404621, 73122)$ and write it as a linear combination; that is, find integers s and t with $d = 7404621s + 73122t$.

Page 57: Exercise 1.58(i): insert absolute value sign:

$$a, b = |ab|,$$

Page 58: Change first two lines of the statement of Theorem 1.40.

Every integer $a \geq 2$ is a prime or a product of primes. Moreover, if a has factorizations

Page 61: Exercise 1.60: insert absolute value sign: $a, b = |ab|$,

Page 66: Insert following line at beginning of the verification of (ii).

Since $1000 = 8 \cdot 125$, we have $1000 \equiv 0 \pmod{8}$, and so

$$1003456789 = 1003456 \cdot 1000 + 789 \equiv 789 \pmod{8}.$$

Page 68: line -5

It follows that $b = sab + tmb$ and $asb \equiv b \pmod{m}$,

Page 73, Exercise 1.74. Replace $x^2 \equiv 1 \pmod{4}$ by $x^2 \equiv 1 \pmod{24}$.

Page 92: lines 19, 20. Change y and Y to x and X .

If $x \in X$, then $x = g(f(x))$, so that $x \in \text{im } g$;

Page 96: add phrase to Exercise 2.7:

... be finite sets, where the x_i are distinct and the y_j are distinct.

Page 101: line 9 should read: gives the 4-cycle $(3\ 7\ 8\ 9)$.

Page 103: replace lines -11 , -10 , -9 with the following:

points, while $\alpha(Y) = Y$. Define $\alpha' = \sigma^{-1}\alpha$, so that $\alpha'(i) = \alpha(i)$ for all $i \in Y$ and α' fixes all $i \notin Y$.

Page 105: Replace line 4 with the following:

It suffices to prove, in any factorization of α into disjoint cycles, that the r -cycles for $r > 1$ are uniquely determined; we prove this statement by induction on ℓ , the larger of t and s . The base

Page 106: line -12 : should read $= (1\ 6)(2\ 4)(3\ 9\ 8\ 7)$.

Page 107: line -6.

$$\gamma = \beta_1\beta_2 \cdots (i_1\ i_2\ \dots) \cdots \beta_t,$$

Page 108: Replace lines 6 through 13 to read as follows:

Assume that γ moves i_1 , say, $\gamma(i_1) = i_2$, so that one of the cycles in the complete factorization of γ is

$$(i_1 i_2 \dots).$$

By definition of σ , one of the cycles in σ is

$$(k \ell \dots),$$

where $\alpha(i_1) = k$ and $\alpha(i_2) = \ell$; hence, $\sigma: k \mapsto \ell$. But $\alpha\gamma\alpha^{-1}: k \mapsto i_1 \mapsto i_2 \mapsto \ell$, and so $\alpha\gamma\alpha^{-1}(k) = \ell = \sigma(k)$. Therefore, σ and $\alpha\gamma\alpha^{-1}$ agree on all symbols of the form $k = \alpha(i_1)$. Since α is surjective, every k is of this form,

Page 111: line 8: change first subscript t to 1:

Definition If $\alpha \in S_n$ and $\alpha = \beta_1 \cdots \beta_t$ is ...

Page 114: Exercise 2.17: change S_{n-1} to S_X , where $X = \{1, \dots, \widehat{j}, \dots, n\}$.

Page 115: In Exercise 2.27, assume that $n \geq 2$.

Page 115: In Exercise 2.29, assume further that none of α , β , and γ is the identity.

Page 126: line 5: exponent should be k :

$$\alpha^k = (\beta_1 \cdots \beta_t)^k = \beta_1^k \cdots \beta_t^k,$$

Page 128: line 8. Change “subgroup” to “a group contained in”

Page 137: Rephrase definition of *cyclic* group:

A group G is called *cyclic* if there is some $a \in G$ with $G = \langle a \rangle$;

Page 140: lines 6 through 10 (= part (iii) of Example)

index has not yet been defined; move these lines to page 141, just above Corollary 2.33.

Page 141: insert part (iii) of Example 2.22 just above statement of Corollary 2.33.

Page 145: line -12 change “the the corresponding” to “the corresponding”

Page 149: line 10. Change “Proposition 2.16” to “Theorem 2.16”

Page 155: In Exercise 2.70, remove the hypothesis G abelian

Pages 155/156: Interchange parts (i) and (ii) in Exercise 2.74.

Page 166: line -6: change LeLeLemma to Lemma

Page 177: In Exercise 2.84(i), add “nonabelian”:

Conclude that the quotient of a nonabelian group by its center ...

Page 177: line -3. Replace H and G/H by $|H|$ and $|G/H|$.

Page 188: line 4. Change “ $n \geq 1$ ” to “ $n \geq 0$ ”

Page 192: line -1. Change “(1 2)(3 4)(5 6)” to “(1 2 3)(4 5 6)”

Page 193: line 3. Change “fixes 1” to “fixes 6”

Page 213: line -7. Change “Theorem 1.53 shows” to “then”

Page 215: lines 1, 2. Replace by

Prove that S may not be a subring of R .

Page 215: Replace Exercise 3.6 by

3.6. Find the inverses of the nonzero elements in \mathbb{Z}_{11} .

Page 215: Exercise 3.13. Change “ a and b ” to “ a and m ”

Page 228: line 18. Change $(s_0, s_1, \dots, s_t, \dots)$ to $(s_0, s_1, \dots, s_i, \dots)$

Page 231: Exercise 3.30(i) should read:

Let R be a domain. Prove that if a polynomial $f(x) \in R[x]$ is a unit, then $f(x)$ is a nonzero constant (the converse is true if R is a field).

Page 238: Exercise 3.44. Assume that p is prime throughout.

Page 238: Exercise 3.49. The definition of multiplication is:

$$(r, s)(r', s') = (rr', ss').$$

Page 241: line 6. Change “ $\text{LF}(f)/\text{LT}(g)$ ” to “ $\text{LT}(f)/\text{LT}(g)$ ”

Page 243: line -3 change “the monic” to “a monic”

line -1: change “The gcd of” to “A gcd of”

Page 246: line 8. Example 3.11(iv) should read:

There are rings other than \mathbb{Z} and $k[x]$ where k is a field, that have a division algorithm; the ring of Gaussian integers $\mathbb{Z}[i]$ is an example of such a ring. These rings are called *euclidean rings*, and they, too, are PID's. We shall consider them at the end of this section.

Page 247: line 4: change “the monic” to “a monic”

line 6: change “The lcm” to “A lcm”

Page 248: line 4. Change “the theorem” to “Proposition 3.32”

Page 250: line -4. Change “ $(\frac{25}{24}5x + \frac{25}{24})$ ” to “ $(\frac{25}{24}5x + \frac{175}{24})$ ”

Page 251: lines 12, 13, 14. Should read

$$\begin{aligned}g &= 1 \cdot f + 2x + 3 \\f &= (3x^2 + 2)(2x + 3).\end{aligned}$$

The gcd is $x - 1$ (which is $2x + 3$ made monic).

Page 259: Exercise 3.58. If k is a field in which $1 + 1 \neq 0$,

Page 260: in Exercise 3.65, assume that fg is monic.

Page 269: line -8. Change $\mathbb{Z}[\alpha] = \langle g_1, \dots, g_m \rangle$ to $\mathbb{Z}[\alpha] = \langle g_1, \dots, g_r \rangle$

Page 270: Replace top 4 lines as follows:

degree m . The additive subgroup A of \mathbb{C} generated by all $\alpha^i \beta^j$, where $0 \leq i < n$ and $0 \leq j < m$, is a finitely generated abelian group containing $\mathbb{Z}[\alpha\beta]$ and $\mathbb{Z}[\alpha + \beta]$ as subgroups. By Exercise 3.80(ii), every subgroup of a finitely generated abelian group is finitely generated, and so both $\alpha\beta$ and $\alpha + \beta$ are algebraic integers, by part (i).

Page 270: line 13 in definition of primitive polynomial should read:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

Page 275: In this list of irreducible cubics over \mathbb{Z}_3 , strike out $x^3 + x^2 + x + 1$ and $x^3 - x - 1$.

Page 278: typo in Exercise 3.79: should read

$$a_n + a_{n-1}x + \dots + a_0x^n.$$

Page 278: add a new Exercise 3.80 (the present Exercise 3.80 on Page 288 should be deleted.)

3.80. Let S be a subgroup of an abelian group A .

(i) If both S and A/S are finitely generated, prove that A is finitely generated.

(ii) Prove that every subgroup S of a finitely generated abelian group A is finitely generated. *Hint.* Use induction on the number of generators of A .

Page 283: line 10: in $K[x]$ is not 1.

Page 283: line 11. whether computed in $K[x]$ or in $k[x]$.

Page 283: line 18, add to the hypothesis of Theorem 3.75 that k is a field.

Page 285: Add to the hypothesis of Theorem 3.77 that $f(x)$ is nonconstant.

Page 286: line 10 should say:

that is, no efficient algorithm is known

Page 286: Rewrite Corollary 3.79 as follows:

Corollary 3.79. Every finite field E has exactly p^n elements for some prime p and some $n \geq 1$.

Proof. Since E is finite, it must have characteristic p for some prime p (see Proposition 3.72); let $k \cong \mathbb{Z}_p$ be its prime field. As E is finite, E^\times is a cyclic group, say, with generator z (by Theorem 3.78). Let $\varphi : k[x] \rightarrow E$ be the homomorphism with $\varphi(x) = z$ and $\varphi(a) = a$ for all $a \in k$ (see the proof of Proposition 3.76). Now φ is surjective, for the powers of z already give all of E^\times , while $\ker \varphi = (q(x))$ for some $q(x) \in k[x]$. By the first isomorphism theorem, $k[x]/(q(x)) \cong E$, and by Example 3.23, $q(x)$ is irreducible in $k[x]$. Finally, Theorem 3.75 shows that every element of E has a unique expression of the form $b_0 + b_1z + \cdots + b_{n-1}z^{n-1}$, where $b_i \in k \cong \mathbb{Z}_p$ and $n = \deg(q)$, which shows that there are exactly p^n elements in E .

Page 288: Delete Exercise 3.80.

Page 309:line –8. Change “Theorem 4.2” to “Proposition 4.2”

Page 332: line –6. Change “[$F(z)/F$]” to “[$F(z) : F$]”

Page 339, line 4 through Page 341, line 12: Delete and replace with following.

We are now going to give an algebraic characterization of constructible numbers.

Definition. A *2-tower* is a tower of subfields of \mathbb{C} ,

$$\mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n,$$

with $[F_j : F_{j-1}] \leq 2$ for all $j \geq 1$. A complex number z is *polyquadratic* if there is a 2-tower $\mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ with $z \in F_n$. Denote the set of all polyquadratic complex numbers by \mathcal{P} .

Note that F/k is a field extension with $[F : k] \leq 2$ if and only if $F = k(u)$, where $u \in F$ is a root of some quadratic polynomial $f(x) \in k[x]$.

Lemma 4.30. (i) \mathcal{P} is a subfield of \mathbb{C} that is closed under square roots.

(ii) A complex number z is polyquadratic if and only if $\operatorname{Re}(z)$ and $\operatorname{Im}(z)$ are polyquadratic.

Proof. (i) If $z, z' \in \mathcal{P}$, then there are 2-towers $\mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ and $\mathbb{Q}(i) = F'_0 \subseteq F'_1 \subseteq \cdots \subseteq F'_m$ with $z \in F_n$ and $z' \in F'_m$. Now $[F_j : F_{j-1}] \leq 2$ implies $F_j = F_{j-1}(u_j)$, where $u_j \in F_j$ is a root of some quadratic $f_j(x) \in F_{j-1}[x]$. For all j with $1 \leq j \leq n$, define $F''_j = F'_m(u_1, \dots, u_j)$. Since $F''_j = F''_{j-1}(u_j)$, we have $F_{j-1} = F'_0(u_1, \dots, u_{j-1}) \subseteq F'_m(u_1, \dots, u_j) = F''_{j-1}$, so that $f_j(x) \in F''_{j-1}[x]$ and $[F''_j : F''_{j-1}] \leq 2$. Hence,

$$\mathbb{Q}(i) = F'_0 \subseteq F'_1 \subseteq \cdots \subseteq F'_m \subseteq F''_1 \subseteq \cdots \subseteq F''_n$$

is a 2-tower. Of course, every element of F_n'' is polyquadratic; since F_n'' contains both z and z' , it contains their inverses and their sum and product. Therefore, \mathcal{P} is a subfield.

Let $z \in \mathcal{P}$. If $\mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ is a 2-tower with $z \in F_n$, then $\mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq F_n(\sqrt{z})$ is also a 2-tower.

(ii) Let $z = a + ib$. If both $a, b \in \mathcal{P}$, then $z = a + ib \in \mathcal{P}$, for \mathcal{P} is a subfield containing i . Conversely, let $\mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ be a 2-tower with $z \in F_n$. Since complex conjugation is an automorphism of \mathbb{C} , $\mathbb{Q}(i) = \overline{F_0} \subseteq \overline{F_1} \subseteq \cdots \subseteq \overline{F_n}$ is a 2-tower with $\overline{z} \in \overline{F_n}$; hence, \overline{z} is polyquadratic. Therefore, $\operatorname{Re}(z) = \frac{1}{2}(z + \overline{z}) \in \mathcal{P}$ and $\operatorname{Im}(z) = \frac{1}{2i}(z - \overline{z}) \in \mathcal{P}$. •

Lemma 4.31. *Let $P = a + ib$, $Q = c + id \in \mathcal{P}$.*

- (i) *The line $L(P, Q)$ has equation $x = a$ if it is vertical [$c = a$] or $y = mx + q$ if it is not vertical [$c \neq a$], where $m, q \in \mathcal{P}$.*
- (ii) *The circle $C(P; Q)$ has equation $(x - a)^2 + (y - b)^2 = r^2$, where $a, b, r \in \mathcal{P}$.*

Proof. Lemma 4.30 gives $a, b, c, d \in \mathcal{P}$.

(i) The statement is clear if $L(P, Q)$ is vertical. If $L(P, Q)$ is not vertical, then its equation is $y = mx + q$, where $m = (d - b)/(c - a)$ and $q = -ma + b$. Hence $m, q \in \mathcal{P}$.

(ii) The circle $C(P; Q)$ has equation $(x - a)^2 + (y - b)^2 = r^2$, where r is the distance from P to Q . Now $a, b \in \mathcal{P}$, by Lemma 4.31, and $r = \sqrt{(c - a)^2 + (d - b)^2} \in \mathcal{P}$, because \mathcal{P} is closed under square roots. •

Proposition 4.32. *Every polyquadratic number z is constructible.*

Proof. If $z \in \mathcal{P}$, then there is a 2-tower $\mathbb{Q}(i) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ with $z \in F_n$; we prove that $z \in K$ by induction on $n \geq 0$. The base step is true, for $F_0 = \mathbb{Q}(i) \subseteq K$, by Theorem 4.29. Now $F_n = F_{n-1}(u)$, where u is a root of a quadratic $f(x) = x^2 + bx + c \in F_{n-1}[x]$. The quadratic formula gives $u \in F_{n-1}(\sqrt{b^2 - 4c})$; but K is closed under square roots, by Theorem 4.29, so that $\sqrt{b^2 - 4c} \in K$. The inductive hypothesis $F_{n-1} \subseteq K$ now gives $z \in F_{n-1}(\sqrt{b^2 - 4c}) \subseteq K(\sqrt{b^2 - 4c}) \subseteq K$. •

Here is the result we have been seeking: an algebraic characterization of a geometric idea.

Theorem 4.33. *A complex number z is constructible if and only if it is polyquadratic.*

Proof. In light of Proposition 4.32: $\mathcal{P} \subseteq K$, it suffices to prove that every constructible z is polyquadratic: $K \subseteq \mathcal{P}$. There are complex numbers $1, w_0 = -1, w_1, \dots, w_m = z$ with w_j constructible from w_0, w_1, \dots, w_{j-1} for all $j \geq 0$. We prove, by induction on $m \geq 0$, that w_m is polyquadratic. Since $w_0 = -1$ is polyquadratic, we may pass to the inductive step. By the inductive hypothesis, we may assume that

w_0, \dots, w_{m-1} are polyquadratic, and so it suffices to prove that if z is constructible from P, Q, R, S , where P, Q, R, S are polyquadratic, then z is polyquadratic.

Case 1: $z \in L(P, Q) \cap L(R, S)$.

If $L(P, Q)$ is vertical, then it has equation $x = a$; if $L(P, Q)$ is not vertical, then Lemma 4.31 says that $L(P, Q)$ has equation $y = mx + q$, where $m, q \in \mathcal{P}$. Similarly, $L(R, S)$ has equation $x = c$ or $y = m'x + p$, where $m', p \in \mathcal{P}$. Since these lines are not parallel, one can solve the linear system

$$\begin{aligned} y &= mx + q \\ y &= m'x + p \end{aligned}$$

for $z = x_0 + iy_0 \in L(P, Q) \cap L(R, S)$. Therefore, $z = x_0 + iy_0 \in \mathcal{P}$.

Case 2: $z \in L(P, Q) \cap C(R; S)$.

If $R = (u, v)$ and $S = (s, t)$, then the circle $C(R; S)$ has equation $(x - u)^2 + (y - v)^2 = \rho^2$, where $\rho^2 = (u - s)^2 + (v - t)^2$; moreover, all coefficients lie in \mathcal{P} , by Lemma 4.31. If the line $L(P, Q)$ is vertical, its equation is $x = a$. If $z = x_0 + iy_0 \in L(P, Q) \cap C(R; S)$, then $(x_0 - u)^2 + (y_0 - v)^2 = \rho^2$, so that y_0 is a root of a quadratic in $\mathcal{P}[x]$, and $z = a + iy_0 \in \mathcal{P}$. If the line $L(P, Q)$ is not vertical, its equation is $y = mx + q$, where $m, q \in \mathcal{P}$. If $z = x_0 + iy_0 \in L(P, Q) \cap C(R; S)$, then $(x_0 - u)^2 + (mx_0 + q - v)^2 = \rho^2$, and so $x_0 \in \mathcal{P}$, for it is a root of a quadratic in $\mathcal{P}[x]$. Hence, $y_0 = mx_0 + q \in \mathcal{P}$ and $z = x_0 + iy_0 \in \mathcal{P}$.

Case 3: $z \in C(P; Q) \cap C(R; S)$.

If $R = (u, v)$ and $S = (s, t)$, the circle $C(R; S)$ has equation $(x - u)^2 + (y - v)^2 = \rho^2$, where $\rho^2 = (u - s)^2 + (v - t)^2$; similarly, if $P = (a, b)$ and $Q = (c, d)$, the circle $C(P; Q)$ has equation $(x - a)^2 + (y - b)^2 = r^2$, where $r^2 = (a - c)^2 + (b - d)^2$. By Lemma 4.31, all the coefficients lie in \mathcal{P} . If $z = x_0 + iy_0 \in C(P; Q) \cap C(R; S)$, then expanding the equations of the circles gives an equation of the form

$$x_0^2 + y_0^2 + \alpha x_0 + \beta y_0 + \gamma = 0 = x_0^2 + y_0^2 + \alpha' x_0 + \beta' y_0 + \gamma'.$$

Canceling $x_0^2 + y_0^2$ gives a linear equation $\lambda x + \mu y + \nu = 0$ with $\lambda, \mu, \nu \in \mathcal{P}$; indeed, $\lambda x + \mu y + \nu = 0$ is the equation of a line $L(P', Q')$ with $P', Q' \in \mathcal{P}$ [for example, take $P' = (0, -\nu/\mu)$ and $Q' = (-\nu/\lambda, 0)$]. Thus, the points $z \in C(P; Q) \cap C(R; S)$ are the points of intersection of the line $L(P', Q')$ and either circle. The argument in Case 2 now shows that $z \in \mathcal{P}$. •

Page 341: line –11 (and index, page 526)

change “M. Hungerbühler” to “N. Hungerbühler”

Page 354: line –1. Change “ ≤ 0 ” to “ < 0 ”

Page 355: lines 1, 2, 3. Make all inequalities strict.

Page 356: line –6. Change “ $x^4 + qx^2 + rs + s$ ” to “ $x^4 + qx^2 + rx + s$ ”

Page 358: Replace line –11 by the following.

$$(x^2 - 2x + 3)(x^2 + 2x - 1).$$

Page 366. Delete lines –9, –8, –7 (last paragraph of the proof of Proposition 4.48)

Page 367: line –16. Change “Theorem 4.48” to “Proposition 4.48”

Page 374: lines 12, 13. Should read:

Proof. Since K is a finite extension, there are elements z_1, \dots, z_ℓ with $K = k(z_1, \dots, z_\ell)$.

Page 375: line 9. Change “ $x^p = a$ ” to “ $x^p - a$ ”

Page 378: line 4. Change “ $\text{Gal}(E/K)$ ” to “ $\text{Gal}(E/k)$ ”

Page 379: line –9. Change “ $(x^3 - x^2 + x + 1)$ ” to “ $(x^3 - x^2 + x - 1)$ ”

Page 379: Rewrite Exercise 4.27 as follows:

4.27. Let k be a field of characteristic p , and define the **Frobenius map** $F: k \rightarrow k$ by $F: a \mapsto a^p$.

(i). Prove that $F: k \rightarrow k$ is an injection.

(ii). When k is finite, prove that F is an automorphism fixing the prime field \mathbb{Z}_p . Conclude that $F \in \text{Gal}(k/\mathbb{Z}_p)$.

(iii). Prove that if k is finite, then every $a \in k$ has a p th root; that is, there is $b \in k$ with $b^p = a$.

Page 380: Exercise 4.29(ii). Change “irrational” to “not rational”

Exercise 4.31(ii). Change “irrational” to “not rational”

Page 387: Replace the proof of (iii) \Rightarrow (i) by:

Since $S_{n+1} \cap (S_1 + S_2 + \dots + S_n) = \{0\}$, we have

$$G = S_{n+1} \oplus (S_1 + S_2 + \dots + S_n).$$

The inductive hypothesis gives $S_1 + S_2 + \dots + S_n = S_1 \oplus S_2 \oplus \dots \oplus S_n$, because, for all $j \leq n$, we have $S_j \cap (S_1 + \dots + \widehat{S}_j + \dots + S_n) \leq S_j \cap (S_1 + \dots + \widehat{S}_j + \dots + S_n + S_{n+1}) = \{0\}$.

Page 392: line –11. and $W = (pG + S)/pG$

Page 393: Add following line at the end of the proof of the Basis Theorem.

Finally, $G = S \oplus T$ implies $d(G) = d(S) + d(T) = 1 + d(T)$, so that $d(T) < d(G)$. By induction, T is a direct sum of cyclic groups, and this completes the proof.

Pages 397 and 398: Replace the last paragraph on page 397 and the first paragraph on page 398 by the following.

Recall that a group G is called *simple* if $G \neq \{1\}$ and G has no normal subgroups other than $\{1\}$ and G itself. We saw, in Proposition 2.78, that the abelian simple groups are precisely the cyclic groups \mathbb{Z}_p of prime order p , and we saw, in Theorem 2.83, that A_n is a nonabelian simple group for all $n \geq 5$. In fact, A_5 is the nonabelian simple group of smallest order. How can one prove that a nonabelian group G of order less than $60 = |A_5|$ is not simple? Exercise 2.105 states that if G is a group of order $|G| = mp$, where p is prime and $1 < m < p$, then G is not simple. This exercise shows that many of the numbers less than 60 are not orders of simple groups. After throwing out all prime powers (p -groups are never nonabelian simple), the only remaining possibilities are

$$12, 18, 24, 30, 36, 40, 45, 48, 50, 54, 56.$$

The solution to the exercise uses Cauchy's theorem, which says that G has a subgroup of order p . We shall see that if G has a subgroup of order p^e instead of p , then Exercise 2.105 can be generalized, and the list of candidates can be shortened. What proper subgroups of G do we know other than cyclic subgroups? The center $Z(G)$ of a group G is a possible candidate, but this subgroup might not be proper or it might be trivial: if G is abelian, then $Z(G) = G$; if $G = S_3$, then $Z(G) = \{1\}$. Hence, $Z(G)$ cannot be used to generalize the exercise.

On pages 403 and 404, replace Lemma 5.20 and Proposition 5.21 by the following.

Lemma 5.20 *There is no nonabelian simple group G of order $|G| = p^e m$, where p is prime, $p \nmid m$, and $p^e \nmid (m-1)!$.*

Proof. Suppose that such a simple group G exists. By Sylow's theorem, G contains a subgroup P of order p^e , hence of index m (notice that the condition $p^e \nmid (m-1)!$ implies $m > 1$). By Theorem 2.67, there exists a homomorphism $\varphi : G \rightarrow S_m$ with $\ker \varphi \leq P$. Since G is simple, however, it has no proper normal subgroups; hence $\ker \varphi = \{1\}$ and φ is an injection; that is, $G \cong \varphi(G) \leq S_m$. By Lagrange's theorem, $p^e m \mid m!$, and so $p^e \mid (m-1)!$, contrary to the hypothesis. •

Lemma 5.21 *There are no nonabelian simple groups of order less than 60.*

Proof. We claim that if p is a prime, then every p -group G with $|G| > p$ is not simple. Theorem 2.75 says that the center, $Z(G)$, is nontrivial. But $Z(G) \triangleleft G$, so that if $Z(G)$ is a proper subgroup, then G is not simple. If $Z(G) = G$, then G is abelian, and Proposition 2.78 says that G is not simple unless $|G| = p$.

The reader may now check that the only integers n between 2 and 59, neither a prime power nor having a factorization of the form $n = p^e m$ as in the statement of the lemma, are $n = 30, 40$, and 56 . By the lemma, these three numbers are the only candidates for orders of nonabelian simple groups of order < 60 .

Assume there is a simple group G of order 30. Let P be a Sylow 5-subgroup of G , so that $|P| = 5$. The number r_5 of conjugates of P is a divisor of 30 and

$r_5 \equiv 1 \pmod{5}$. Now $r_5 \neq 1$ lest $P \triangleleft G$, so that $r_5 = 6$. By Lagrange's theorem, the intersection of any two of these is trivial (intersections of Sylow subgroups can be more complicated; see Exercise 5.10). There are 4 nonidentity elements in each of these subgroups, and so there are $6 \times 4 = 24$ nonidentity elements in their union. Similarly, the number r_3 of Sylow 3-subgroups of G is 10 (for $r_3 \neq 1$, r_3 is a divisor of 30, and $r_3 \equiv 1 \pmod{3}$). There are 2 nonidentity elements in each of these subgroups, and so the union of these subgroups has 20 nonidentity elements. We have exceeded the number of elements in G , and so G cannot be simple.

Next, assume there is a simple group G of order 56. If P is a Sylow 7-subgroup of G , then P must have $r = 8$ conjugates (for $r \mid 56$ and $r \equiv 1 \pmod{7}$). Since these groups are cyclic of prime order, the intersection of any pair of them is $\{1\}$, and so there are 48 nonidentity elements in their union. Thus, adding the identity, we have accounted for 49 elements of G . Now a Sylow 2-subgroup Q has order 8, and so it contributes 7 more nonidentity elements, giving 56 elements. But there is a second Sylow 2-subgroup, lest $Q \triangleleft G$, and we have exceeded our quota. Therefore, there is no simple group of order 56.

We dispose of simple groups G of order 40 in several stages. First, we show that the only normal subgroups N of S_5 are $\{1\}$, A_5 , and S_5 . Suppose that $N \triangleleft S_5$ is neither A_5 nor S_5 . By the second isomorphism theorem, $N \cap A_5 \triangleleft A_5$, so that simplicity of A_5 gives $N \cap A_5 = \{1\}$ or $N \cap A_5 = A_5$. The latter case forces $A_5 \leq N$; that is, $N = A_5$ or $N = S_5$, contradicting our assumption; hence, $N \cap A_5 = \{1\}$. Now suppose there is $\alpha \in N$ with $\alpha \neq (1)$; if $\beta \in N$ and $\beta \neq (1)$, then both α and β are odd, because $N \cap A_5 = \{1\}$, and so $\alpha\beta = (1)$, because odd \times odd = even. Hence, $\beta = \alpha^{-1}$, and $|N| \leq 2$. But $|N| = 2$ cannot happen, for neither $\langle (a\ b) \rangle$ nor $\langle (a\ b)(c\ d) \rangle$ is a normal subgroup of S_5 . Therefore, $N = \{1\}$. (The same argument shows, for all $n \geq 5$, that the only normal subgroups of S_n are $\{1\}$, A_n , and S_n .) Second, we show that S_5 has no subgroup H of order 40. Otherwise, representing S_5 on the cosets of H gives a homomorphism $\rho: S_5 \rightarrow S_3$ with $\ker \rho \leq H$; that is, $\ker \rho \triangleleft S_5$ and $|\ker \rho| \leq 40$. The first stage shows that $\ker \rho = \{1\}$, and this gives $S_5 \cong S_3$, a contradiction. Finally, if G is a simple group of order 40, then a Sylow 2-subgroup P of G has order 8, hence index 5, and so $G \rightarrow S_5$, the representation on the cosets of P , is an injection, because G is simple; that is, S_5 has a subgroup of order 40. This contradiction shows that no simple group of order 40 can exist. •

Page 407: Exercise 5.12. Change “UT(3, 2)” to “UT(3, \mathbb{Z}_2)”

Page 431: line 17. Change the definition of A .

$$A = \begin{bmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{bmatrix}.$$

Page 431: line -5

$$\text{and } BAB^{-1} = \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix}.$$

Page 457: line 13 that is, there is some $I_0 \in \mathcal{F}$ for which there is no $J \in \mathcal{F}$ with $I_0 < J$.

Page 505: hint to 1.10(iii) should read:

$$\sum_{i=1}^n \left(\sum_{p=1}^i p \right) = \frac{1}{2} \sum_{i=1}^n i^2 + \frac{1}{2} \sum_{i=1}^n i.$$

Page 510: hint to 2.60 should be changed so that

$$f(x/(x-1)) = (1\ 3) \quad \text{and} \quad f((x-1)/x) = (1\ 3\ 2).$$