***Errata for Advanced Modern Algebra, Chapters 1 to 7***

***March 7, 2003***

This list of errors will be corrected in the next printing of the book. If you have found any other mistakes – typos, errors in a proof, false statements, unclear exposition, important omission – please write me at

rotman@math.uiuc.edu

***Page 12***, line 2 Change formula to

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

***Page 12***, line 6 Change "$f^{(n)}$" to "$(fg)^{(n)}$"

***Page 12***, line $-9$ Change Exercise 1.14 as follows:

**1.14** If $r, a) = 1 = (r', a)$, prove that $(rr', a) = 1$.

***Page 14***, line 15 Should read: "$10 \equiv -1 \bmod 11$"

***Page 14***, line $-11$ Delete "on page 14"

***Page 20***, line 13 Change "$0, 1, \ldots, k-1$." to "$0, 1, \ldots, n-1$."

***Page 21***, lines 9, 10 Change the definition.

**Definition**. Define the ***Euler $\phi$-function*** as the degree of the $n$th cyclotomic polynomial:

$$\phi(n) = \deg(\Phi_n(x)).$$

***Page 41***, line $-7$ Should read: "$\alpha\colon 1 \mapsto 6$."

***Page 49***, line $-6, -5$ Add 1-cycles (12) and (16), and calculate $\operatorname{sgn}(\alpha) = (-1)^{16-5}$.

***Page 58***, line $-12$ Change "Theorem 2.33(i)" to "Theorem 2.24"

***Page 60***, line 5 The beginning of a sentence was omitted. It begins

(ii) The symmetry group $\Sigma(\pi_5)$ of a regular pentagon ...

***Page 62***, The hint for Exercise 2.23 should refer to Theorem 2.24

***Page 65***, line 10 Change "**Proposition 1.18**" to "**Proposition 1.19**"

***Page 65***, line $-7$ Change "by (i)," to "by Theorem 2.24,"

***Page 68***, lines 3 and 4 Change "$\{\mathbf{v} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{0}\}$" to "$\{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} = \mathbf{0}\}$"

***Page 70***, line $-13$ Change the reference from Exercise 1.19 to the new Exercise 1.14.

***Page 74***, lines $-12, -11$ Change "3, 4" to "4, 5"

***Page 79***, line $-13$ A finite nonabelian group is called ***hamiltonian***

***Page 82***, Exercise 2.59 Change "$M^2 = -E$" to "$M^2 = -I$"

***Page 82***, Exercise 2.60 Change "$\mathbf{ij} = -\mathbf{ki}$" to "$\mathbf{ik} = -\mathbf{ki}$"

***Page 83***, line $-11$ Change "Let $gk \in bK$" to "Let $gk \in gK$"

***Page 86***, line $-9$ Change "Theorem 2.33(i)" to "Theorem 2.24"

***Page 87***, line $-93$ Change "$d \mapsto (hd, d^{-1}h)$" to "$d \mapsto (hd, d^{-1}k)$"

***Page 88***, line 17 Change "$aK = H$" to "$aH = H$"

***Page 90*** Restate Proposition 2.78 to read as follows.

*If $G$ is a finite abelian group and $d$ is a divisor of $|G|$, then $G$ contains a subgroup of order $d$.*

The present proof proves this result when $d$ is a prime, and the following paragraph completes the proof.

Let $d$ be any divisor of $|G|$, and let $p$ be a prime divisor of $d$. We have just seen that there is a subgroup $S \leq G$ of order $p$. Now $S \lhd G$, because $G$ is abelian, and $G/S$ is a group of order $n/p$. By induction on $|G|$, $G/S$ has a subgroup $H^*$ of order $d/p$. The correspondence theorem gives $H^* = H/S$ for some subgroup $H$ of $G$ containing $S$, and $|H| = |H^*||S| = d$ $\bullet$.

***Page 91***, line 15 Delete "$= hh'kk'$"

***Page 92***, line 20 Change "Theorem 2.33(i)" to "Theorem 2.24"

***Page 93***, line 15 Change "[Theorem 2.33(i)]" to "[Theorem 2.24]"

***Page 94***, line $-9$ Leep's proof assumes that the group $G$ is abelian. This enters in the proof to ensure that $\theta$ is a homomorphism.

***Page 101***, line -13 Change "$N_G(x) = \{g \in G : gHg^{-1} \leq H\}$" to "$N_G(H) = \{g \in G : gHg^{-1} = H\}$"

***Page 104***, line -9 Change "$n \geq 1$" to "$n \geq 0$"

***Page 113*** Replace Exercise 2.88.

**2.88** Find $N_G(H)$ if $G = S_4$ and $H = \langle(1\ 2\ 3)\rangle$.

***Page 113*** Change Exercise 2.91 to read

**2.91** For all $n \geq 5$, prove that all 3-cycles are conjugate in $A_n$.

***Page 115*** Change the formula on the bottom line to read:

$$\tfrac{1}{12}\left(q^6 + 2q^4 + 4q^3 + 3q^2 + 2q\right)$$

***Page 125***, Exercise 3.19(i) Stochastic matrices should all be nonsingular.

***Page 129***, lines -5 to -3 Change "Lemma 3.15(iii)" to "Proposition 3.14"

***Page 134***, lines $-5, -4, -3$ Should read:

element of each of them is known. For example, finding a primitive element of $\mathbb{F}_{257}$ essentially involves checking the powers of each $[i]$, where $1 < i < 257$, until one is found for which $i^m \not\equiv 1 \bmod 257$ for all positive integers $m < 256$.

***Page 141***, line $-4$ Change "Exercise 1.15(ii)" to "Exercise 1.15(i)"

***Page 150***, line 2 Change "Example 3.15" to "Example 3.45(i)"

***Page 150***, line 8 Assume that $\varphi$ is injective.

***Page 150***, lines -5, -4 Rewrite as follows:

Prove that $F$ is a field (with operations matrix addition and matrix multiplication), and prove that there is an isomorphism $\varphi\colon F \to \mathbb{C}$ with $\det(A) = \varphi(A)\overline{\varphi(A)}$.

***Page 154***, line 6 Change "or" to "and" in the display.

***Page 155***, line 18 Change "$m$ mod 4" to "$m$ mod $p$"

***Page 156***, bottom Change the statement of Proposition 3.68:

*Let $\alpha = a + bi \in \mathbb{Z}[i]$ be neither 0 nor a unit. Then $\alpha$ is irreducible if and only if*

(i) *$\alpha$ is an associate of a prime $p$ in $\mathbb{Z}$ of the form $p = 4m + 3$; or*

(ii) *$\alpha$ is an associate of $1 + i$ or its conjugate $1 - i$; or*

(iii) *$\partial\alpha = a^2 + b^2$ is a prime in $\mathbb{Z}$ of the form $4m + 1$.*

***Page 157*** Redo part (iii) of the proof as follows:

If $\partial(\alpha)$ is a prime $p$ (with $p \equiv 1 \bmod 4$), then $\alpha$ is irreducible, by Proposition 3.64(ii). Conversely, suppose $\alpha$ is irreducible. As $\partial(\alpha) = p$ or $\partial(\alpha) = p^2$, it suffices to eliminate the latter possibility. Now $\alpha \mid p$, so that $p = \alpha\beta$ for some $\beta \in \mathbb{Z}[i]$; hence, as in case (i), $\partial(\alpha) = p^2$ implies that $\beta$ is a unit. Now $\alpha\overline{\alpha} = p^2 = (\alpha\beta)^2$, so that $\overline{\alpha} = \alpha\beta^2$. But $\beta^2 = \pm 1$, by Proposition 3.64(iii), contradicting $\overline{\alpha} \neq \pm\alpha$. Therefore, $\partial(\alpha) = p$. •

***Page 158*** Change Exercise 3.61 as follows:

**3.61** If $k$ is a field, prove that $k[[x]]$, the ring of formal power series over $k$, is a PID. (See Exercises 3.26 and 3.27 on page 130.)

***Page 163***, line 4 Should read: "finite list in $V$"

***Page 166***, line 9, Change "re-ordering the $u$'s" to "re-ordering the $v$'s"

***Page 173*** Change the sketch of proof of Proposition 3.94.

If $e_1, \ldots, e_n$ is the standard basis of $k^n$, define $P$ to be the matrix whose $i$th column is the coordinate set of $T(e_i)$. If $S\colon k^n \to k^n$ is defined by $S(y) = Py$, then $S = T$ because both agree on a basis: $T(e_i) = \sum_j a_{ji}e_j = Pe_i$.

***Page 174***, line 4, Change "$m \times 1$ column" to "$n \times 1$ column"

***Page 175***, line 2, Change "$w_i = \sum$" to "$z_i = \sum$"

***Page 175***, line 3, insert $T(v_i) = z_i$

***Page 181***, line -7, complete the definition of the column space as the subspace of $k^m$ spanned by the columns of $A$

***Page 183***, line 12, Change "Corollary 2.52" to "Corollary 2.69"

***Page 185***, Change the statement of Proposition 3.116

*If $k$ is a field and $I = (p(x))$, where $p(x)$ is a nonzero polynomial in $k[x]$, then the following are equivalent: $p(x)$ is irreducible; $k[x]/I$ is a field; $k[x]/I$ is a domain.*

***Page 188***, line -10, Change "$\varphi(c) = c + I$" to "$\varphi(c + I) = c$"

***Page 189***, line 7, Change "$\varphi(c) = c + I$" to "$\varphi(c + I) = c$"

***Page 189***, line 8, Change "$\varphi^{-1}\psi$" to "$\psi\varphi^{-1}$"

***Page 191***, line 19, Change "$f(x) \in k[x]$" to "$f(x) \in K[x]$"

***Page 192***, line 13, Change "Frac($k[y_1, \ldots, y_n]$)" to "Frac($k[y_1, \ldots, y_n]$)[$x$]"

***Page 192***, line -16, Change "if $K$ contains" to "if $k$ contains"

***Page 193***, line 15, Should be $E = \{\alpha \in K : g(\alpha) = 0\}$;

***Page 194***, lines -11 and -2, Change "Corollary 3.129(v)" to "Corollary 3.117(v)"

***Page 196***, line -1, Change "$(x^3 - x^2 + 1)$" to "$(x^3 - x^2 - 1)$"

***Page 197***, Change Exercise 3.85 (which repeats Exercise 3.33).

**3.85** If $X$ is a subset of a commutative ring $R$, define $\mathcal{I}(X)$ to be the intersection of all those ideals $I$ in $R$ that contain $X$. Prove that $\mathcal{I}(X)$ is the set of all $a \in R$ for which there exist finitely many elements $x_1, \ldots, x_n \in X$ and elements $r_i \in R$ with $a = r_1x_1 + \cdots + r_nx_n$.

***Page 197***, Add new exercise.

**3.95** Let $K/k$ be a field extension. If $A \subseteq K$ and $u \in k(A)$, prove that there are $a_1, \ldots, a_n \in A$ with $u \in k(a_1, \ldots, a_n)$.

***Page 202***, Change the first sentence of Theorem 4.17(i):

(i) *Let $E/k$ be a splitting field of a separable polynomial $f(x) \in$*

***Page 202***, Change the first sentence of Theorem 4.17(ii):

(ii) *If $E/k$ is a splitting field of a separable polynomial $f(x) \in k[x]$, then*

***Page 204***, line -8 Change "Now $E^\times = \langle\omega\rangle$," to "The group of all roots of $x^m - 1$ is cyclic, say, with generator $\omega$,"

***Page 205***, line 17 Add new sentence at end.

By Theorem 3.131, Gal$(E/k)$ is independent of the choice of splitting field $E$.

***Page 205***, line 22 Change "$z_i$" to "$z_1$"

***Page 205***, line 8 Delete: "it is a deep theorem of L. Kronecker and H. Weber that"

***Page 208***, line -13 Add the following

[note that $h^3$ is also a root of this quadratic, so that $h^3 = \frac{1}{2}(-r - \sqrt{R})$].

***Page 208***, line -3 Change "$\mathbb{R}[x]$" to "$\mathbb{Q}[x]$"

***Page 208***, line -2 Change "$\mathbb{Q}(q, r)$" to "$\mathbb{Q}$"

***Page 211***, Change the statement of Lemma 4.17(ii) to read

(ii) *If $K/k$ is a radical extension, then the extension $E/k$ constructed in part (i) is also a radical extension.*

***Page 212***, line 10 Add "where $p_i \neq char(K_0)$,"

***Page 212***, line -9 Change "By Proposition 4.11," to "By Theorem 4.7(ii)"

***Page 213***, line 18 Add "where $p_i \neq char(k)$,"

***Page 214***, line 18 Replace lines 7, 8, 9 by following.

the last equation holding because $G_i G_{i+1} = G_i$. Since $G_{i+1} \lhd G_i \cap G_{i+1}N$, the third isomorphism theorem gives a surjection $G_i/G_{i+1} \to G_i/[G_i \cap G_{i+1}N]$, and so the composite is a surjection $G_i/G_{I+1} \to G_i N/G_{i+1}N$. As $G_i/G_{i+1}$ is cyclic of

***Page 215***, line -5 Replace "Proposition 4.21" by "Lemma 4.20"

***Page 218***, Replace Exercise 4.11 by the following

**4.11** Let $k$ be a field, let $f(x) \in k[x]$ be a separable polynomial of prime degree $p$, and let $E/k$ be a splitting field. Prove that Gal$(E/k) \cong \mathbb{I}_p$ implies that $f(x)$ is irreducible.

***Page 224***, line 4 Change "its normal closure" to "the radical extension constructed in Lemma 4.17"

***Page 224***, line 13 Change "$e_{n-j}$" to "$e_j$"

***Page 225***, line 17 Change "If $\beta \in k(S)$, there are" to "If $\alpha \in k(S)$, then (*new*) Exercise 3.95 on page 197 says that there are"

***Page 227***, Replace the proof of Lemma 4.42 as follows.

*Proof.* Since $a, b \preceq a \vee b$, we have $\varphi(a \vee b) \preceq \varphi(a), \varphi(b)$; that is, $\varphi(a \vee b)$ is a lower bound of $\varphi(a), \varphi(b)$. It follows that $\varphi(a \vee b) \preceq \varphi(a) \wedge \varphi(b)$.

For the reverse inequality, surjectivity of $\varphi$ gives $c \in \mathcal{L}$ with $\varphi(a) \wedge \varphi(b) = \varphi(c)$. Now $\varphi(c) = \varphi(a) \wedge \varphi(b) \preceq \varphi(a), \varphi(b)$. Applying $\varphi^{-1}$, which is also order-reversing, we have $a, b \preceq c$. Hence, $c$ is an upper bound of $a, b$, so that $a \vee b \preceq c$. Therefore,

$\varphi(a \vee b) \succeq \varphi(c) = \varphi(a) \wedge \varphi(b)$. A similar argument proves the other half of the statement. •

***Page 228***, lines 3 and 5. Interchange Int$(E/k)$ and Sub(Gal$(E/k)$)

***Page 228***, line -9. Change "$E/E^{\mathrm{Gal}(E/B)}$" to "$E/B$"

***Page 232***, lines 18, 19 Change "$n+1$" to "$n-1$" 4 times

***Page 232***, lines -3, -2 Replace sentence beginning "By the fundamental" with

By the fundamental theorem of symmetric polynomials ([*new*] Exercise 6.84 on page 410), there is a polynomial $\varphi(x) \in \mathbb{R}[x_1, \ldots, x_n]$ with

***Page 233***, lines -13, -12 Replace "Hence $[E : \mathbb{C}] =$ ... if $m - 1 \geq 1$, this" by

Now $E/\mathbb{C}$ is also a Galois extension, and Gal$(E/\mathbb{C}) \leq G$ is also a 2-group. If this group is nontrivial, then it has a subgroup $H$ of index 2. By the fundamental theorem of Galois theory, the intermediate field $E^H$ is an extension of $\mathbb{C}$ of degree 2, and this

***Pages 235, 236*** In the proof of Theorem 4.53, replace the last two lines on page 235 and first 13 lines on page 236:

*Proof.* Since $G$ is solvable, it has a normal subgroup $H$ of prime index, say, $p$. Let $\omega$ be a primitive $p$th root of unity, which exists in some extension field $k^*$, because $k$ has characteristic 0. We distinguish two cases.

Case (i): $\omega \in k$.

We prove the statement by induction on $[E : k]$. The base step is obviously true, for $k = E$ is a radical extension of itself. For the inductive step, consider the intermediate field $E^H$. Now $E/E^H$ is a Galois extension, by Corollary 4.36, and Gal$(E/E^H)$ is solvable, being a subgroup of the solvable group $G$. Since $[E : E^H] < [E : k]$, the inductive hypothesis gives a radical tower

$$E^H \subseteq R_1 \subseteq \cdots \subseteq R_t,$$

where $E \subseteq R_t$. Now $E^H/k$ is a Galois extension, because $H \lhd G$, and its index $[G : H] = p = [E^H : k]$, by the fundamental theorem. In this case, Corollary 4.51 (or Proposition 4.52) applies to give $E^H = k(z)$, where $z^p \in k$; that is, $E^H/k$ is a pure extension. Hence, the radical tower above can be lengthened by adding the prefix $k \subseteq E^H$, thus displaying $R_t/k$ as a radical extension.

Case (ii): General case.

***Page 237***, line 4 Change "$k(x)$" to "$k[x]$"

***Pages 237, 238***, Replace the proof of Proposition 4.56.

*Proof.* Let $\alpha$ be a root of $f(x)$. It is easy to see that the roots of $f(x)$ are $\alpha + i$, where $0 \leq i < p$, for Fermat's theorem gives $i^p = i$ in $\mathbb{F}_p$, and so

$$(\alpha + i)^p - (\alpha + i) - t = \alpha^p + i^p - \alpha - i - t = \alpha^p - \alpha - t = 0.$$

It follows that $f(x)$ is a separable polynomial and that $k(\alpha)$ is a splitting field of $f(x)$ over $k$. We claim that $f(x)$ is irreducible in $k[x]$. Suppose that $f(x) = g(x)h(x)$, where

$$g(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0 \in k[x]$$

and $0 < d < \deg(f) = p$; then $g(x)$ is a product of $d$ factors of the form $\alpha + i$. Now $-c_{d-1} \in k$ is the sum of the roots: $-c_{d-1} = d\alpha + j$, where $j \in \mathbb{F}_p$, and so $d\alpha \in k$. Since $0 < d < p$, however, $d \neq 0$ in $k$, and this forces $\alpha \in k$, contradicting the lemma. Therefore, $f(x)$ is an irreducible polynomial in $k[x]$. Since $\deg(f) = p$, we have $[k(\alpha) : k] = p$ and, since $f(x)$ is separable, we have $|\operatorname{Gal}(k(\alpha)/k)| = [k(\alpha) : k] = p$. Therefore, $\operatorname{Gal}(k(\alpha)/k) \cong \mathbb{I}_p$.

It will be convenient to have certain roots of unity available. Let $\Omega$ be the set of all $q$th roots of unity, where $q < p$ is a prime divisor of $p!$. We claim that $\alpha \notin k(\Omega)$. On the one hand, if $n = \prod_{q<p} q$, then $\Omega$ is contained in the splitting field of $x^n - 1$, and so $[k(\Omega) : k] \mid n!$, by Theorem 4.3. It follows that $p \nmid [k(\Omega) : k]$. On the other hand, if $\alpha \in k(\Omega)$, then $k(\alpha) \subseteq k(\Omega)$ and $[k(\Omega) : k] = [k(\Omega) : k(\alpha)][k(\alpha) : k] = p[k(\Omega) : k(\alpha)]$. Hence, $p \mid [k(\Omega) : k]$, and this is a contradiction.

If $f(x)$ were solvable by radicals over $k(\Omega)$, there would be a radical extension

$$k(\Omega) = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_r$$

with $k(\Omega, \alpha) \subseteq B_r$. We may assume, for each $i \geq 1$, that $B_i/B_{i-1}$ is of prime type; that is, $B_i = B_{i-1}(u_i)$, where $u_i^{q_i} \in B_{i-1}$ and $q_i$ is prime. There is some $j \geq 1$ with $\alpha \in B_j$ but $\alpha \notin B_{j-1}$. Simplifying notation, we set $u_j = u$, $q_j = q$, $B_{j-1} = B$, and $B_j = B'$. Thus, $B' = B(u)$, $u^q = b \in B$, $\alpha \in B'$, and $\alpha, u \notin B$. We claim that $f(x) = x^p - x - t$, which we know to be irreducible in $k[x]$, is also irreducible in $B[x]$. By accessory irrationalities, Exercise 4.5 on page 217, restriction gives an injection $\operatorname{Gal}(B(\alpha)/B) \to \operatorname{Gal}(k(\alpha)/k)) \cong \mathbb{I}_p$. If $\operatorname{Gal}(B(\alpha)/B) = \{1\}$, then $B(\alpha) = B$ and $\alpha \in B$, a contradiction. Therefore, $\operatorname{Gal}(B(\alpha)/B) \cong \mathbb{I}_p$, and $f(x)$ is irreducible in $B[x]$, by (*new*) Exercise 4.11 on page 218.

Since $u \notin B'$ and $B$ contains all the $q$th roots of unity, Proposition 3.126 shows that $x^q - b$ is irreducible in $B[x]$, for it does not split in $B[x]$. Now $B' = B(u)$ is a splitting field of $x^q - b$, and so $[B' : B] = q$. We have $B \subsetneq B(\alpha) \subseteq B'$, and

$$q = [B' : B] = [B' : B(\alpha)][B(\alpha) : B].$$

Since $q$ is prime, $[B' : B(\alpha)] = 1$; that is, $B' = B(\alpha)$, and so $q = [B' : B]$. As $\alpha$ is a root of the irreducible polynomial $f(x) = x^p - x - t \in B[x]$, we have $[B(\alpha) : B] = p$; therefore, $q = p$. Now $B(u) = B' = B(\alpha)$ is a separable extension, by Proposition 4.38, for $\alpha$ is a separable element. It follows that $u \in B'$ is also a separable element, contradicting $\operatorname{irr}(u, B) = x^q - b = x^p - b = (x - u)^p$ having repeated roots.

We have shown that $f(x)$ is not solvable by radicals over $k(\Omega)$. It follows that $f(x)$ is not solvable by radicals over $k$, for if there were a radical extension $k = R_0 \subseteq R_1 \subseteq \cdots \subseteq R_t$ with $k(\alpha) \subseteq R_t$, then $k(\Omega) = R_0(\Omega) \subseteq R_1(\Omega) \subseteq \cdots \subseteq R_t(\Omega)$ would show that $f(x)$ is solvable by radicals over $k(\Omega)$, a contradiction. •

***Page 238***, line -2 Change "$u_i$" and "$u_j$" to "$\alpha_i$" and "$\alpha_j$"

***Page 240***, line 7 Change "$\alpha_i - \frac{1}{n}c_{n-1}$" to "$\alpha_i + \frac{1}{n}c_{n-1}$"

***Page 240***, line -3 Add the phrase

(we saw on page 208 that $g^3 - h^3 = \sqrt{R}$)

***Page 241***, line -7 Should read: "$Let\ f(x) \in \mathbb{Q}[x]$"

***Page 242***, line 12 Should read: "$x^3 - 2$ is irreducible in $\mathbb{Q}[x]$"

***Page 242***, line -7 Delete: "that is, if these fields are linearly disjoint"

***Page 246***, Exercise 4.19(iii): Change "$[L \wedge K$" to "$[L \vee K$"

***Page 257***, line 10 Change "$t \in T$" to "$v \in T$"

***Page 257*** Replace the first 8 lines of the proof of Lemma 5.15 by:

*Proof.* Since $G$ is finite, we may choose an element $y \in G$ of largest order, say, $p^\ell$. We claim that $S = \langle y \rangle$ is a pure subgroup of $G$.

Suppose that $s \in S$, so that $s = mp^t y$, where $t \geq 0$ and $p \nmid m$, and let

$$s = p^n a$$

for some $a \in G$; an element $s' \in S$ must be found with $s = p^n s'$. We may assume that $n < \ell$: otherwise, $s = p^n a = 0$ (for $p^\ell g = 0$ for all $g \in G$ because $y$ has largest order $p^\ell$), and we may choose $s' = 0$.

If $t \geq n$, define $s' = mp^{t-n} y \in S$, and note that

$$p^n s' = p^n m p^{t-n} y = mp^t y = s.$$

***Page 259***, line$-6$ Change "$x_i$" to "$x$"

***Page 262***, line 1 Define $x_n = x$

***Page 263***, line 1 Change "2.79" to "5.7"

***Page 266*** Replace the last paragraph of the proof of Theorem 5.32 with the following.

To prove isomorphism, it suffices, by the fundamental theorem, to prove that the elementary divisors can be computed from the invariant factors. Since $c_j = p_1^{e_{1j}} p_2^{e_{2j}} \cdots p_n^{e_{nj}}$, the fundamental theorem of arithmetic shows that $c_j$ determines all those prime powers $p_i^{e_{ij}}$ which are distinct from 1; that is, the invariant factors $c_j$ determine the elementary divisors. •

In Example 5.31, we started with elementary divisors and computed invariant factors.

Let us now start with invariant factors and compute elementary divisors.

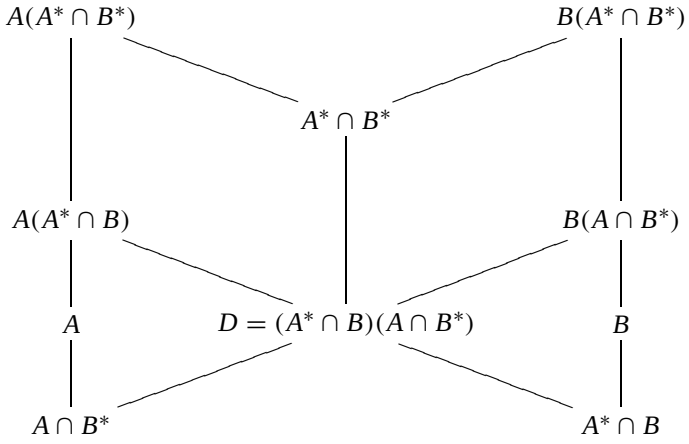
$$\begin{aligned} \text{invariant factors} &\leftrightarrow \text{elementary divisors} \\ 2 \mid 6 \mid 6 = 2 \mid 2 \cdot 3 \mid 2 \cdot 3 &\leftrightarrow (2,2,2,3,3) \\ 6 \mid 12 = 2 \cdot 3 \mid 2^2 \cdot 3 &\leftrightarrow (2,4,3,3) \\ 3 \mid 24 = 3 \mid 2^3 \cdot 3 &\leftrightarrow (8,3,3) \\ 2 \mid 2 \mid 18 = 2 \mid 2 \mid 2 \cdot 3^2 &\leftrightarrow (2,2,2,9) \\ 2 \mid 36 = 2 \mid 2^2 \cdot 3^2 &\leftrightarrow (2,4,9) \\ 72 = 2^3 \cdot 3^2 &\leftrightarrow (8,9). \end{aligned}$$

***Page 269***, line -9 Change "$aGa^{-1}$" to "$a^{-1}Ga$"

***Page 277***, line 5 Change "ayy" to "a"

***Page 279*** Add to the remark:

The Zassenhaus lemma is sometimes called the *butterfly lemma* because of the following picture. I confess that I have never liked this picture; it doesn't remind me of a butterfly, and it doesn't help me understand or remember the proof.




***Page 279***, line -8 Replace the sentence beginning with "Note that $\varphi$" by

Now $\varphi$ is well-defined: if $ax = a'x'$, where $a' \in A$ and $x' \in A^* \cap B^*$, then $(a')^{-1}a = x'x^{-1} \in A \cap (A^* \cap B^*) = A \cap B^* \leq D$; also, $\varphi$ is a homomorphism: $axa'x' = a''xy$, where $a'' = a(xa'x^{-1}) \in A$ (because $A \lhd A^*$), and so $\varphi(axa'x') = \varphi(a''xx') = xx'D = \varphi(ax)\varphi(a'x')$.

***Page 281*** lines $-11, -9, -7$ Change "refinement" to "subsequence"

***Page 281*** line $-6$ Insert after $N_{j+1} \lhd N_j$,

says both subsequences are normal series, hence are refinements, and there is

***Page 288*** Delete the finiteness in all three parts of Exercise 5.47

***Page 289***, line −14 Change "$[K, L, h]$" to "$[K, L, H]$"

***Page 289***, line −10 Should read:

the three subgroups lemma with $L = \zeta^2(G)$ and $H = K = G$.

***Page 290***, line 3 Should read "where $r \in k$ and $r \neq 0$"

***Page 291***, line 16 Change "$(q^2 - q)(q^2 - q)$" to "$(q^2 - 1)(q^2 - q)$"

***Page 292***, line 9 Change "$|\operatorname{SL}(2, \mathbb{F}_q)|$" to "$|\operatorname{PSL}(2, \mathbb{F}_q)|$"

***Page 292*** In Lemma 5.64, drop the hypothesis that $H$ contains the center.

***Page 295***, line 5 Change "$-2v = -2ub \neq 0$" to "$-2v = 6ub = 4ub \neq 0$"

***Page 295***, line -16 Should read: "all the nonabelian simple groups"

***Page 296***, Change the hint for Exercise 5.53:

**Hint**. Let $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 1 & 1+u \\ 0 & 1 \end{smallmatrix}\right]$, where $u \in \mathbb{F}_9$ satisfies $u^2 = -1$. If $A$ and $B$ represent elements $a$ and $b$ in $\operatorname{PSL}(2, \mathbb{F}_9)$, prove that $ab$ has order 5 and $|\langle a, b\rangle| = 60$.

***Page 301***, line 1 Change "If $u \sim v$ and $u' \sim v'$" to "If $u \sim u'$ and $v \sim v'$"

***Page 302*** Replace last 10 lines of proof of Proposition 5.71 by the following.

The only ways the deletion of $bb^{-1}$ can occur in the second instance is if, in $w_{j-1} = XY$, we have $X = X'b$ or $Y = b^{-1}Y'$. If $X = X'b$, then $w_{j-1} = X'bY$ and $w_j = X'bb^{-1}bY$ (and it will be the subword $bb^{-1}$ that will be deleted by the elementary operation $w_i \to w_{i+1}$). As with the first possibility, we do not need the insertion. In more detail, the chain

$$X'bY \to X'bb^{-1}bY \to \cdots \to Abb^{-1}C \to A'aa^{-1}A''bb^{-1}C \to A'aa^{-1}A''C,$$

where the processes $X' \to A$ and $bY \to C$ involve insertions only, can be shortened by removing the insertion of $b^{-1}b$:

$$X'bY \to \cdots \to AC \to A'aa^{-1}A''C.$$

The second case, $Y = b^{-1}Y'$, is treated in the same way. Therefore, in all cases, we are able to shorten the shortest chain, and so no such chain can exist. •

***Page 305*** The map $g'$ was not defined in the proof of Lemma 5.74.

Define $g'\colon F/F' \to G$ by $wF' \mapsto g(w)$ ($g'$ is well-defined because $G$ abelian forces $F' \leq \ker g$).

***Page 307*** Replace the statement and proof of von Dyck's theorem:

**Theorem 5.78** (**von Dyck's Theorem**). Let a group $G$ have a presentation

$$G = (x_1, \ldots, x_n \mid r_j,\ j \in J);$$

that is, $G = F/N$, where $F$ is free on $\{x_1, \ldots, x_n\}$ and $N$ is the normal subgroup of $F$ generated by all $r_j = r_j(x_1, \ldots, x_n)$. If $H = \langle h_1, \ldots, h_n \rangle$ is a group and if $r_j(h_1, \ldots, h_n) = 1$ in $H$ for all $j \in J$, then there is a surjective homomorphism $G \to H$ with $x_i N \mapsto h_i$ for all $i$.

*Proof.* If $F$ is the free group with basis $\{x_1, \ldots, x_n\}$, then there is a homomorphism $\varphi\colon F \to H$ with $\varphi(x_i) = h_i$ for all $i$. Since $r_j(h_1, \ldots, h_n) = 1$ in $H$ for all $j \in J$, we have $r_j \in \ker\varphi$ for all $j \in J$, which implies $N \leq \ker\varphi$. Therefore, $\varphi$ induces a (well-defined) homomorphism $G = F/N \to H$ with $x_i N \mapsto h_i$ for all $i$. •

***Page 307*** Change the definition so that

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

This leads to two more changes:

$$A^{2^i} = \begin{bmatrix} \omega^{2^i} & 0 \\ 0 & \omega^{-2^i} \end{bmatrix} \qquad \text{and} \qquad BAB^{-1} = \begin{bmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{bmatrix}.$$

***Page 310***, line 10 Change "15" to "14"

***Page 311*** The correct spelling is Nielsen

***Page 315/316*** Replace the last paragraph of the proof of Theorem 5.88 (bottom 4 lines of page 315, top 2 lines of page 316).

If $\varepsilon = -1$, then the definition of coset functions gives

$$(x^{-1})^{Su} = (x^{Sux^{-1}})^{-1} = (y_{Sux^{-1},x})^{-1}.$$

Hence,

$$\varphi((x^{-1})^{Su}) = (t_{Sux^{-1},x})^{-1} = [\ell(Sux^{-1})x\ell(Sux^{-1}x)]^{-1} = [\ell(Sux^{-1})x\ell(Su)]^{-1}.$$

Since $\ell$ is a Schreier transversal, we have $\ell(Su) = u$ and $\ell(Sux^{-1}) = \ell(Sv) = v = ux^{-1}$. Hence,

$$\varphi((x^{-1})^{Su}) = [(ux^{-1})xu^{-1}]^{-1} = 1.$$

Therefore, $y_{Sux^{-1},x}$ is special, $(x^{-1})^{Su} \in T$, and the proof is complete. •

***Page 316/317*** Replace the bottom of the proof of Corollary 5.91, starting on line -5, ending on page 317.

Since $Sb \neq S$, we have $\ell(Sb) = b = ux^{\varepsilon}$; since $\ell$ is a Schreier transversal, we have $u \in \ell$. Define $\psi(Sb)$ as follows.

$$\psi(Sux^{\varepsilon}) = \begin{cases} (Su, x) & \text{if } \varepsilon = +1; \\ (Sux^{-1}, x) & \text{if } \varepsilon = -1. \end{cases}$$

Note that $\psi(Sux^{\varepsilon})$ is a trivial ordered pair. If $\varepsilon = +1$, then $\ell(Sux) = \ell(Sb) = b = ux$, so that $\ell(Su)x = ux$ and $t_{Su,x} = 1$. If $\varepsilon = -1$, then $\ell(Sbx) = \ell(Sux^{-1}x) = \ell(Su) = u$, so that $\ell(Sb)x = bx = ux^{-1}x = u$ and $t_{Sb,x} = 1$.

To see that $\psi$ is injective, suppose that $\psi(Sb) = \psi(Sc)$, where $b = ux^{\varepsilon}$ and $c = vy^{\eta}$; we assume that $x, y$ lie in the given basis of $F$ and that $\varepsilon = \pm 1$ and $\eta = \pm 1$. There are four possibilities, depending on the signs of $\varepsilon$ and $\eta$.

$$(Su, x) = (Sv, y),\ (Su, x) = (Svy^{-1}, y);\ (Sux^{-1}, x) = (Sv, y);\ (Su, x) = (Svy^{-1}, y).$$

In every case, equality of ordered pairs gives $x = y$. If $(Su, x) = (Sv, x)$, then $Su = Sv$, hence, $Sb = Sux = Svx = Sc$, as desired. If $(Su, x) = (Svx^{-1}, x)$, then $Su = Sc$, and so $\ell(Su) = \ell(Sc) = c$. But $\ell(Su)x = \ell(Sux) = b$, because $(Su, x)$ is a trivial ordered pair. Hence, $b = \ell(Su)x = cx = vx^{-1}x$, contradicting $b$ (as any element of a Schreier transveral) being reduced. A similar contradiction shows that we cannot have $(Sux^{-1}, x) = (Sv, x)$. Finally, if $(Sux^{-1}, x) = S(vx^{-1}, x)$, then $Sb = Sux^{-1} = Svx^{-1} = Sc$.

To see that $\psi$ is surjective, take a trivial ordered pair $(Sw, x)$; that is, $\ell(Sw)x = wx = \ell(Sux)$. Now $w = ux^{\varepsilon}$, where $u \in \ell$ and $\varepsilon = \pm 1$. If $\varepsilon = +1$, then $w$ does not end with $x^{-1}$, and $\psi(Swx) = (Sw, x)$. If $\varepsilon = -1$, then $w$ does end with $x^{-1}$, and so $\psi(Su) = (Sux^{-1}, x) = (Sw, x)$. •

***Page 318*** Change Exercise 5.72

**5.72** Let $Y$ and $S$ be groups, and let $\varphi\colon Y \to S$ and $\theta\colon S \to Y$ be homomorphisms with $\varphi\theta = 1_S$.

(i) If $\rho\colon Y \to Y$ is defined by $\rho = \theta\varphi$, prove that $\rho\rho = \rho$ and $\rho(a) = a$ for every $a \in \operatorname{im}\theta$. (The homomorphism $\rho$ is called a ***retraction***.)

(ii) If $K$ is the normal subgroup of $Y$ generated by all $y^{-1}\rho(y)$ for $y \in Y$, prove that $K = \ker\varphi$.

**Hint**. Note that $\ker\varphi = \ker\rho$, for $\theta$ is an injection. Use the equation $y = \rho(y)(\rho(y)^{-1})y$ for all $y \in Y$.

***Page 319***, line -4 Change "$(a) \subseteq (b)$" to "$(b) \subseteq (a)$"

***Page 323***, line -3 Delete the parenthetical remark.

***Page 325***, Delete part (i) of Exercise 6.4.

***Page 325***, Add a new part to Exercise 6.10.

(iii) Let $P$ be a prime ideal and $Q_1, \dots, Q_r$ be ideals. Prove that if $Q_1 \cap \cdots \cap Q_r \subseteq P$, then $Q_i \subseteq P$ for some $i$.

***Page 326***, Exercise 6.15 Should read: "Exercise 8.21 on page 533"

***Page 329***, line 19 Replace "$(b)$" by "$(r)$"

***Page 331***, line -5 Rewrite the definition of content and then move it to the next page, after the new version of Lemma 6.24.

**Definition**. If $R$ is a UFD with $Q = \mathrm{Frac}(R)$, and if $f(x) \in Q[x]$, then $f(x) = df^*(x)$, where $d \in Q$ and $f^*(x) \in R[x]$ is primitive. We call $d$ the ***content*** of $f(x)$, writing $d = c(f)$, and we call $f^*(x)$ the ***associated primitive polynomial***.

***Page 332***, Replace the statement of Lemma 6.24 as follows.

**Lemma 6.24**. *Let $R$ be a* UFD, *let $Q = \mathrm{Frac}(R)$, and let $f(x) \in Q[x]$ be nonzero.*

(i) *There is a factorization*

$$f(x) = df^*(x),$$

*where $d \in Q$ and $f^*(x) \in R[x]$ is primitive. This factorization is unique in the sense that if $f(x) = rg^*(x)$, where $r \in Q$ is nonzero and $g^*(x) \in R[x]$ is primitive, then $f^*(x)$ and $g^*(x)$ are associates in $R[x]$ and there is a unit $w \in R$ with $wd = r$.*

(ii) *If $f(x), g(x) \in R[x]$, then $c(fg)$ and $c(f)c(g)$ are associates in $R$ and $(fg)^*$ and $f^*g^*$ are associates in $R[x]$.*

(iii) *Let $f(x) \in Q[x]$ have a factorization $f(x) = dg^*(x)$, where $d \in Q$ and $g^*(x) \in R[x]$ is primitive. Then $f(x) \in R[x]$ if and only if $d \in R$.*

(iv) *Let $g^*(x),\ f(x) \in R[x]$. If $g^*(x)$ is primitive and $g^*(x) \mid bf(x)$, where $b \in R$ and $b \neq 0$, then $g^*(x) \mid f(x)$.*

***Page 334*** Here is new proof of part (i)

Clearing denominators, there is $b \in R$ with $bf(x) \in R[x]$. Define $f^*(x) = (b/c)\,f(x)$, where $c$ is the content of $bf(x)$. Now $f^*(x)$ is primitive, for $c$ is the gcd of the coefficients of $bf(x)$, and $f(x) = (c/b)\,f^*(x)$.

To prove uniqueness, suppose that $df^*(x) = f(x) = rg^*(x)$, where $d, r \in Q$ and $f^*(x), g^*(x) \in R[x]$ are primitive. Exercise 6.17 on page 339 allows us to write $r/d$ in lowest terms: $r/d = u/v$, where $u$ and $v$ are relatively prime elements of $R$. The equation $vf^*(x) = ug^*(x)$ holds in $R[x]$; equating like coefficients, $v$ is a common divisor of each coefficient of $ug^*(x)$. Since $u$ and $v$ are relatively prime, Exercise 6.18(i) on page 339 gives $v$ a common divisor of the coefficients of $g^*(x)$. But $g^*(x)$ is primitive, and so $v$ is a unit. A similar argument shows that $u$ is a unit. Therefore, $r/d = u/v$ is a unit in $R$, call it $w$; we have $wd = r$ and $f^*(x) = wg^*(x)$, as desired.

***Page 334*** Here is new proof of part (iii)

If $d \in R$, then it is obvious that $f(x) = dg^*(x) \in R[x]$. Conversely, if $f(x) \in R[x]$, then $f(x) = c(f)\,f^*(x)$, where $c(f) \in R$ is the content of $f(x)$. By uniqueness, there is a unit $w \in R$ with $d = wc(f) \in R$.

***Page 335***, line 15 Add: "namely, $m(x) = \mathrm{irr}(\alpha, \mathbb{Q})$,"

***Page 338***, line 14 Change "UFD" to "PID"

***Page 339*** Change the proof of Corollary 6.37.

Let $R = k[x_1, \cdots, x_n]$. Note that $f$ is primitive in $R[y]$, because $(g, h) = 1$ forces any divisor of its coefficients $g, h$ to be a unit. Since $f$ is linear in $y$, it is not the product

of two polynomials in $R[y]$ of smaller degree, and hence Corollary 6.36 shows that $f$ is irreducible in $R[y] = k[x_1, \ldots, x_n, y]$.

***Page 342***, line 7 Change "$I_N = J$" to "$I_n = J$"

***Page 343***, line 1 Change "$J$" to "$I$' (two times)

***Page 351*** Replace the second paragraph of the proof of Theorem 6.53

Suppose that $ab \in I$ but $a \notin I$ and $b \notin I$. Since $a \notin I$, the ideal $I + Ra$ is strictly larger than $I$, and so $I + Ra$ is finitely generated; indeed, we may assume that

$$I + Ra = (i_1 + r_1 a, \ldots, i_n + r_n a),$$

where $i_k \in I$ and $r_k \in R$ for all $k$. Consider $J = (I : a) = \{x \in R : xa \in I\}$. Now $I + Rb \subseteq J$; since $b \notin I$, we have $I \subsetneq J$, and so $J$ is finitely generated. We claim that $I = (i_1, \ldots, i_n, Ja)$. Clearly, $(i_1, \ldots, i_n, Ja) \subseteq I$, for every $i_k \in I$ and $Ja \subseteq I$. For the reverse inclusion, if $z \in I \subseteq I + Ra$, there are $u_k \in R$ with $z = \sum_k u_k(i_k + r_k a)$. Then $(\sum_k u_k r_k)a = z - \sum_k u_k i_k \in I$, so that $\sum_k u_k r_k \in J$. Hence, $z = \sum_k u_k i_k + (\sum_k u_k r_k)a \in (i_1, \ldots, i_n, Ja)$. It follows that $I = (i_1, \ldots, i_n, Ja)$ is finitely generated, a contradiction, and so $I$ is a prime ideal.

***Page 354***, line 14 Should read "Exercise 9.93 on page 755."

***Page 355***, line -8 Replace the proof of Corollary 6.59 by:

If $k$ is countable, then the set $T$ of all nonconstant polynomials is countable, for $k[x]$ is countable. Hence, $k[T]$ is countable, as is its quotient $k_1$ (in the proof of Theorem 6.58). It follows, by induction on $n \geq 0$, that every $k_n$ is countable. Finally, a countable union of countable sets is itself countable, so that an algebraic closure of $k$ is countable.

***Page 357***, line 4 Change the second display

$$f_0^*(p(x)) = \prod_{i=1}^{n}(x - b_i),$$

where $f_0^*\colon E_o[x] \to \overline{k}[x]$ is the map induced by $f_0$.

***Page 358***, line 4 Should read: "Now $\varphi(x) \in k(x)$ has"

***Page 358***, lines 7 – 11 Replace paragraph

If $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}(2, k)$, write $\langle A\rangle = (ax+b)/(cx+d)$. If we define $\langle A'\rangle\langle A\rangle = \langle A'A\rangle$, then it is easily checked that the set $\mathrm{LF}(k)$ of all linear fractional transformations with entries in $k$ is a group under this operation. In Exercise 6.57 on page 375, the reader will prove that $\mathrm{LF}(k) \cong \mathrm{PGL}(2, k) = \mathrm{GL}(2, k)/Z(2, k)$, where $Z(2, k)$ is the (normal) subgroup of all $2 \times 2$ (nonzero) scalar matrices.

***Pages 359 - 360*** Replace Lüroth's theorem.

**Theorem 6.66** (**Lüroth's Theorem**). *If $k(x)$ is a simple transcendental extension, then every intermediate field $B$ is also a simple transcendental extension of $k$: There is $\varphi \in B$ with $B = k(\varphi)$.*

*Proof.* If $\beta \in B$ is not constant, then $[k(x) : k(\beta)] = [k(x) : B][B : k(\beta)]$ is finite, by Proposition 6.63; hence, $[k(x) : B]$ is finite and $x$ is algebraic over $B$. The proof of Proposition 6.63 shows that if $\varphi \in k(x)$, then $\varphi$ is a coefficient of $\mathrm{irr}(x, k(\varphi))$; the proof of Lüroth's theorem is a converse, showing that $B = k(\varphi)$ for some coefficient $\varphi$ of $\mathrm{irr}(x, B)$. Now

$$\mathrm{irr}(x, B) = y^n + \beta_{n-1}y^{n-1} + \cdots + \beta_0 \in B[y].$$

Each coefficient $\beta_\ell \in B \subseteq k(x)$ is a rational function, which we write in lowest terms: $\beta_\ell = g_\ell(x)/h_\ell(x)$, where $g_\ell(x), h_\ell(x) \in k[x]$ and $(g_\ell, h_\ell) = 1$. As in Lemma 6.24(i), the content $c(\mathrm{irr}) = d(x)/b(x)$, where $b(x)$ is the product of the $h_\ell$ and $d(x)$ is their gcd. It is easy to see that $f(x)$, defined by $f(x) = b(x)/d(x)$, lies in $k[x]$; in fact, the reader may generalize Exercise 1.26 on page 13 to show that $f(x)$ is the lcm of the $h_\ell$. Define

$$i(x, y) = f(x)\,\mathrm{irr}(x, B),$$

the associated primitive polynomial in $k[x][y]$ (of course, $k[x][y] = k[x, y]$, but we wish to view it as polynomials in $y$ with coefficients in $k[x]$). If we denote the highest exponent of $y$ occurring in a polynomial $a(x, y)$ by $\deg_y(a)$, then $n = \deg_y(i)$; let $m = \deg_x(i)$. Since $i(x, y) = f(x)y^n + \sum_{\ell=0}^{n-1} f(x)\beta_\ell y^\ell$, we have $m = \max_\ell\{\deg(f), \deg(f\beta_\ell)\}$. Now $h_\ell(x) \mid f(x)$ for all $\ell$, so that $\deg(h_\ell) \le \deg(f) \le m$ [because $f(x)$ is one of the coefficients of $i(x, y)$]. Also,

$$f\beta_\ell = \frac{h_0 \cdots h_{n-1}}{d} \cdot \frac{g_\ell}{h_\ell} = \frac{h_0 \cdots \widehat{h}_\ell \cdots h_{n-1}}{d} g_\ell.$$

Since $(h_0 \cdots \widehat{h}_\ell \cdots h_{n-1})/d \in k[x]$, we have $\deg(g_\ell) \le \deg(f\beta_\ell) \le m$. We conclude that $\deg(g_\ell) \le m$ and $\deg(h_\ell) \le m$.

Some coefficient $\beta_j$ of $\mathrm{irr}(x, B)$ is not constant, lest $x$ be algebraic over $k$. Omit the subscripts $j$, write $\beta_j = g(x)/h(x)$, and define

$$\varphi = \beta_j = g(x)/h(x) \in B.$$

Now $g(y) - \varphi h(y) = g(y) - g(x)h(x)^{-1}h(y) \in B[y]$ has $x$ as a root, and so $\mathrm{irr}(x, B)$ divides $g(y) - \varphi h(y)$ in $B[y] \subseteq k(x)[y]$. Therefore, there is $q(x, y) \in k(x)[y]$ with

$$\mathrm{irr}(x, B)q(x, y) = g(y) - \varphi h(y). \tag{1}$$

Since $g(y) - \varphi h(y) = h(x)^{-1}\big(h(x)g(y) - g(x)h(y)\big)$, the content $c\big(g(y) - \varphi h(y)\big)$ is $h(x)^{-1}$ and the associated primitive polynomial is

$$\Phi(x, y) = h(x)g(y) - g(x)h(y).$$

Notice that $\Phi(x, y) \in k[x][y]$ and that $\Phi(y, x) = -\Phi(x, y)$.

Rewrite Eq. (1), where $c(q) \in k(x)$ is the content of $q(x, y)$:

$$f(x)^{-1} i(x, y) c(q) q(x, y)^* h(x) = \Phi(x, y)$$

(remember that $f(x)^{-1}$ is the content of $\mathrm{irr}(x, B)$ and $i(x, y)$ is its associated primitive polynomial). The product $i(x, y)q(x, y)^*$ is primitive, by Gauss's Lemma 6.23. But $\Phi(x, y) \in k[x][y]$, so that Lemma 6.24(iii) gives $f(x)^{-1}c(q)h(x) \in k[x]$. We now define $q^{**}(x, y) = f(x)^{-1}c(q)h(x)q(x, y)$, so that $q^{**}(x, y) \in k[x, y]$ and

$$i(x, y)q^{**}(x, y) = \Phi(x, y) \quad \text{in } k[x, y]. \tag{2}$$

Let us compute degrees in Eq. (2): the degree in $x$ of the left hand side is

$$\deg_x(iq^{**}) = \deg_x(i) + \deg_x(q^{**}) = m + \deg_x(q^{**}), \tag{3}$$

while the degree in $x$ of the right hand side is

$$\deg_x(\Phi) = \max\{\deg(g), \deg(h)\} \leq m, \tag{4}$$

as we saw above. We conclude that $m + \deg_x(q^{**}) \leq m$, so that $\deg_x(q^{**}) = 0$; that is, $q^{**}(x, y)$ is a function of $y$ alone. But $\Phi(x, y)$ is a primitive polynomial in $x$, and hence the symmetry $\Phi(y, x) = -\Phi(x, y)$ shows that it is also a primitive polynomial in $y$. Thus, $q^{**}$ is a constant, and so $i(x, y)$ and $\Phi(x, y)$ are associates in $k[x, y]$; hence, $\deg_x(\Phi) = \deg_x(i) = m$. With Eq. (4), this equality gives

$$m = \deg_x(\Phi) = \max\{\deg(g), \deg(h)\}.$$

Symmetry of $\Phi$ also gives $\deg_y(\Phi) = \deg_x(\Phi)$, and so

$$n = \deg_y(\Phi) = \deg_x(\Phi) = m = \max\{\deg(g), \deg(h)\}.$$

By definition, $\mathrm{degree}(\varphi) = \max\{\deg(g), \deg(h)\} = m$; hence, Proposition 6.63 gives $[k(x) : k(\varphi)] = m$. Finally, since $\varphi \in B$, we have $[k(x) : k(\varphi)] = [k(x) : B][B : k(\varphi)]$. As $[k(x) : B] = n = m$, this forces $[B : k(\varphi)] = 1$; that is, $B = k(\varphi)$. •

***Page 362***, lines -3 to -1 Replace with following.

the exchange axiom. If $x \preceq S$ and $x \not\preceq S - \{y\}$, then $S = S' \cup \{y\}$ with $y \notin S'$. There are scalars $a_i, a$ with $x = ay + \sum_i a_i s_i$, where $s_i \in S'$; since $x \notin \langle S' \rangle$, we must have $a \neq 0$. Therefore, $y = a^{-1}(x - \sum_i a_i s_i) \in \langle S', x \rangle$, and so $y \preceq S' \cup \{x\}$.

***Page 363***, lines 6 - 8 Replace text beginning with "In light" by

Using this notation, $x \preceq S$ if and only if $x \in \overline{k(S)}$. Moreover, $s \preceq T$ for every $s \in S$ says that $S \subseteq \overline{k(T)}$. It follows that $x \in \overline{k(T)}$, by Lemma 6.56(i), and so $x \preceq T$.

***Page 363***, line 14 Change "$k(S)[y]$" to "$k(S, u)[y]$"

***Page 363***, Add text and replace Lemma 6.70.

By Proposition 6.67, algebraic independence defined on page 361 coincides with independence just defined for the dependency relation in Lemma 6.69.

**Lemma 6.70**. *Let $\preceq$ be a dependency relation on a set $\Omega$. If $T \subseteq \Omega$ is independent and $z \not\preceq T$ for some $z \in \Omega$, then $T \cup \{z\} \supsetneq T$ is a strictly larger independent subset.*

*Proof.* Since $z \not\preceq T$, axiom (i) gives $z \notin T$, and so $T \subsetneq T \cup \{z\}$; it follows that $(T \cup \{z\}) - \{z\} = T$. If $T \cup \{z\}$ is dependent, then there exists $t \in T \cup \{z\}$ with $t \preceq (T \cup \{z\}) - \{t\}$. If $t = z$, then $z \preceq T \cup \{z\} - \{z\} = T$, contradicting $z \not\preceq T$. Therefore, $t \in T$. Since $T$ is independent, $t \not\preceq T - \{t\}$. If we set $S = T \cup \{z\} - \{t\}$, $t = x$, and $y = z$ in the exchange axiom, we conclude that $z \preceq (T \cup \{z\} - \{t\}) - \{z\} \cup \{t\} = T$, contradicting the hypothesis $z \not\preceq T$. Therefore, $T \cup \{z\}$ is independent. •

***Page 365***. Place Theorem 6.73 after the definition of transcendence basis.

***Pages 366*** Change (iii) of Proposition 6.76 to read:

(iii) *If $k$ is a field of characteristic $p > 0$ and if $f'(x) = 0$, then $f(x)$ has no repeated roots. Conversely, if $f(x)$ is an irreducible polynomial in $k[x]$, then the conditions in parts* (i) *and* (ii) *are all equivalent.*

***Pages 366–367*** Rewrite Corollary 6.77.

**Corollary 6.77**. *If $k$ is a field of characteristic $p > 0$ and $f(x) \in k[x]$, then there exists $e \geq 0$ and a polynomial $g(x) \in k[x]$ with $g(x) \notin k[x^p]$ and $f(x) = g(x^{p^e})$. Moreover, if $f(x)$ is irreducible, then $g(x)$ is separable.*

*Proof.* If $f(x) \notin k[x^p]$, define $g(x) = f(x)$; if $f(x) \in k[x^p]$, there is $f_1(x) \in [x]$ with $f(x) = f_1(x^p)$. Note that $\deg(f) = p \deg(f_1)$. If $f_1(x) \notin k[x^p]$, define $g(x) = f_1(x)$; otherwise, there is $f_2(x) \in k[x]$ with $f_1(x) = f_2(x^p)$; that is,

$$f(x) = f_1(x^p) = f_2(x^{p^2}).$$

Since $\deg(f) > \deg(f_1) > \cdots$, iteration of this procedure must end after a finite number $e$ of steps. Thus, $f(x) = g(x^{p^e})$, where $g(x)$, defined by $g(x) = f_e(x)$, does not lie in $k[x^p]$. If, now, $f(x)$ is irreducible, then $f_1(x)$ is irreducible, for a factorization of $f_1(x)$ would give a factorization of $f(x)$. It follows that $f_i(x)$ is irreducible for all $i$. In particular, $f_e(x)$ is irreducible, and so it is separable, by Proposition 6.76(iii). •

***Page 369***, lines 5 - 10 Replace by the following.

Therefore, $h_1(x)$ is constant; absorbing it into $g_1(x)$, we have $x^{p^{e-1}} - c = g_1(x)$ and

$$x^{p^e} - c = g_1(x^p) = g(x)^m.$$

If $p \mid m$, then $x^{p^e} - c = (g(x)^p)^{m/p}$, and so all the coefficients lie in $k^p$, contradicting $c \notin k^p$; therefore, $p \nmid m$. Equation (5) now gives $g'(x) = 0$, so that $g(x) \in k[x^p]$; say,

$g(x) = g_2(x^p)$. This forces $m = 1$, because $x^{p^e} - c = g(x)^m$ gives $x^{p^{e-1}} - c = g_2(x)^m$, which is a forbidden factorization of the irreducible $x^{p^{e-1}} - c$. •

***Page 369*** The proof of Proposition 6.81 is garbled. Borrow part of Corollary 6.83, so it looks as follows.

**Proposition 6.81**.

(i) *Let $k \subseteq B \subseteq E$ be a tower of fields with $E/k$ algebraic. If $E/k$ is separable, then $E/B$ is separable.*

(ii) *Let $E/k$ be an algebraic field extension, where $k$ has characteristic $p > 0$. If $E/k$ is a separable extension, then $E = k(E^p)$. Conversely, if $E/k$ is finite and $E = k(E^p)$, then $E/k$ is separable.*

*Proof.* (i) If $\alpha \in E$, then $\alpha$ is algebraic over $B$, and $\text{irr}(\alpha, B) \mid \text{irr}(\alpha, k)$ in $B[x]$, for their gcd is not 1 and $\text{irr}(\alpha, B)$ is irreducible. Since $\text{irr}(\alpha, k)$ has no repeated roots, $\text{irr}(\alpha, B)$ has no repeated roots, and hence $\text{irr}(\alpha, B)$ is a separable polynomial. Therefore, $E/B$ is a separable extension.

(ii) Let $E/k$ be a separable extension. Now $k(E^p) \subseteq E$, and so $E/k(E^p)$ is a separable extension, by part (i). But if $\beta \in E$, then $\beta^p \in E^p \subseteq k(E^p)$; say, $\beta^p = \alpha$. Hence, $\text{irr}(\beta, k(E^p)) \mid (x^p - \alpha)$ in $\big(k(E^p)\big)[x]$, and so this polynomial is not separable because it divides $x^p - \alpha = (x - \beta)^p$. We conclude that $\beta \in k(E^p)$; that is, $E = k(E^p)$.

Conversely, suppose that $E = k(E^p)$. We begin by showing that if $\beta_1, \ldots, \beta_s$ is a linearly independent list in $E$ (where $E$ is now viewed only as a vector space over $k$), then $\beta_1^p, \ldots, \beta_s^p$ is also linearly independent over $k$. Extend $\beta_1, \ldots, \beta_s$ to a basis $\beta_1, \ldots, \beta_n$ of $E$, where $n = [E : k]$. Now $\beta_1^p, \ldots, \beta_n^p$ spans $E^p$ over $k^p$, for if $\eta \in E$, then $\eta = \sum_i a_i \beta_i$, where $a_i \in k$, and hence $\eta^p = \sum_i a_i^p \beta_i^p$. Now take any element $\gamma \in E$. Since $E = k(E^p)$, we have $\gamma = \sum_j c_j \eta_j$, where $c_j \in k$ and $\eta_j \in E^p$. But $\eta_j = \sum_i a_{ji}^p \beta_i^p$ for $a_{ji} \in k$, as we have just seen, so that $\gamma = \sum_i \left( \sum_j c_j a_{ji}^p \right) \beta_i^p$; that is, $\beta_1^p, \ldots, \beta_n^p$ spans $E$ over $k$. Since $\dim_k(E) = n$, this list is a basis, and hence its sublist $\beta_1^p, \ldots, \beta_s^p$ must be linearly independent over $k$.

Since $E/k$ is finite, each $\alpha$ is algebraic over $k$. If $\text{irr}(\alpha, k)$ has degree $m$, then $1, \alpha, \alpha^2, \ldots, \alpha^m$ is linearly dependent over $k$, while $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ is linearly independent. If $\alpha$ is inseparable, then $\text{irr}(\alpha, k) = f_e(x^{p^e})$ and $m = p^e r$ where $r$ is the reduced degree of $\text{irr}(\alpha, k)$. Since $r = m/p^e < m$, we have $1, \alpha, \alpha^2, \ldots, \alpha^r$ linearly independent over $k$. But $\alpha^{p^e}$ is a root of $f_e(x)$, so there is a nontrivial dependency relation on $1, \alpha^{p^e}, \alpha^{2p^e}, \ldots, \alpha^{rp^e}$ (for $rp^e = m$). We have seen, in the preceding paragraph, that linear independence of $1, \alpha, \alpha^2, \ldots, \alpha^r$ implies linear independence of $1, \alpha^{p^e}, \alpha^{2p^e}, \ldots, \alpha^{rp^e}$. This contradiction shows that $\alpha$ must be separable over $k$. •

***Page 370*** lines -2, -1. Should read,

a ***purely inseparable extension*** if $E/k$ is algebraic and, for every $\alpha \in E$, there is $e \geq 0$ with $\alpha^{p^e} \in k$.

If $E/k$ is a purely inseparable extension and $B$ is an intermediate field, then it is clear that $E/B$ is purely inseparable.

***Page 371*** Add a phrase to Proposition 6.85.

**Proposition 6.85**. *If $E/k$ is an algebraic field extension, then $E/E_s$ is a purely inseparable extension. Moreover, if $\alpha \in E$, then* $\operatorname{irr}(\alpha, E_s) = x^{p^m} - c$ *for some* $m \geq 0$.

*Proof.* If $\alpha \in E$, write $\operatorname{irr}(\alpha, k) = f_e(x^{p^e})$, where $e \geq 0$ and $f_e(x) \in k[x]$ is a separable polynomial. It follows that $\alpha^{p^e}$ is separable over $k$ and $\alpha^{p^e} \in E_s$. If $\alpha \notin E_s$, choose $m$ minimal with $\alpha^{p^m} \in E_s$. Now $\alpha$ is a root of $x^{p^m} - \alpha^{p^m}$, which is irreducible, by Lemma 6.80, and so $\operatorname{irr}(\alpha, E_s) = x^{p^m} - c$, where $c = \alpha^{p^m}$. •

***Page 371*** line -12 Delete "by Proposition 6.85,"

***Page 372*** line 13 Should read $b_i^{p^e} \in B_s$

***Page 372*** line 14 Should read

the list $b_1^{p^e} \dots b_r^{p^e}$ is linearly dependent over $B_s$, contradicting Corollary 6.82 (for $E_s/B_s$

***Page 372*** line 13 Should read "But $E_s/B$"

***Page 391***, Corollary 6.83 now reads as follows.

**Corollary 6.83**. *If $k \subseteq B \subseteq E$ is a tower of algebraic extensions, then $B/k$ and $E/B$ are separable extensions if and only if $E/k$ is a separable extension.*
*Proof.* Since $B/k$ and $E/B$ are separable, Proposition 6.81(ii) gives $B = k(B^p)$ and $E = B(E^p)$. Therefore,

$$E = B(E^p) = k(B^p)(E^p) = k(B^p \cup E^p) = k(E^p) \subseteq E,$$

because $B^p \subseteq E^p$. Therefore, $E/k$ is separable, by Proposition 6.81(ii).

Conversely, if every element of $E$ is separable over $k$, we have, in particular, that each element of $B$ is separable over $k$; hence, $B/k$ is a separable extension. Finally, Proposition 6.81(i) shows that $E/B$ is a separable extension. •

***Page 391***, line -14 Rewrite the definition:

***Page 393***, line 16 Replace "Thus, $Q$ is" by "Thus, $Q = (x^2, y)$ is"

**Definition**. An ideal $Q$ is ***primary*** if it is a proper ideal and if $ab \in Q$ (where $a, b \in R$) and $b \notin Q$, then $a^n \in Q$ for some $n \geq 1$.

***Page 394***, Replace lines 1, 2 as follows:

must stop (because $R/J$, being a quotient of the noetherian ring $R$, is itself noetherian); there is $m \geq 1$ with $\ker(a_{R/J}^{\ell}) = \ker(a_{R/J}^{m})$ for all $\ell \geq m$. Denote $(a_{R/J})^m$ by $\varphi$, so that $\ker(\varphi^2) = \ker\varphi$. Note

***Page 394***, Replace lines 6, 7, 8 by

$$\ker\varphi \cap \operatorname{im}\varphi = \{0\}.$$

If $x \in \ker\varphi \cap \operatorname{im}\varphi$, then $\varphi(x) = 0$ and $x = \varphi(y)$ for some $y \in R/J$. But $\varphi(x) = \varphi(\varphi(y)) = \varphi^2(y)$, so that $y \in \ker(\varphi^2) = \ker\varphi$ and $x = \varphi(y) = 0$.

***Page 394***, line -9 Remove subscript $i$ from $P_i$

***Page 394***, line -6 Remove radical from $\sqrt{(I : c_i)}$

***Page 394***, line -4 Should read

if $ab \in (I : c)$ and $a \notin (I : c)$, then $b \in P_i$ and $(I : c)$ is $P_i$-primary.

***Page 395***, Replace lines 11 and 12 by

If $c \in Q_i$, then $(Q_i : c) = R$; if $c \notin Q_i$, then we saw, in first part of this proof, that $(Q_i : c)$ is $P_i$-primary. Thus, there is $s \leq r$ with

$$P = \sqrt{(Q_{i_1} : c)} \cap \cdots \cap \sqrt{(Q_{i_s} : c)} = P_{i_1} \cap \cdots \cap P_{i_s}.$$

Of course, $P \subseteq P_{i_j}$ for all $j$. On the other hand, Exercise 6.10(iii) on page 325 (new exercise) gives $P_{i_j} \subseteq P$ for some $j$, and so $P = P_{i_j}$, as desired. •

***Page 404***, line $-8$ Change "Write" to "Define"

***Page 404***, line $-2$ Change "$\prec_{\text{lex}}$" to "$\preceq_{\text{lex}}$"

***Page 406***, line 3 Should read

(ii) Let $h(X) = cX^{\gamma} + \text{lower terms}$ and let $g(X) = bX^{\beta} + \text{lower terms}$, so that $\text{LT}(h) =$

***Page 410*** Add a second part to Exercise 6.79.

(ii) Prove that $\text{Deg}(fg) = \text{Deg}(f) + \text{Deg}(g)$, and $\text{Deg}(f^m) = m\,\text{Deg}(f)$ for all $m \geq 1$.

***Page 411*** Add a new exercise.

**6.84** Let $f(X) = \sum_{\alpha} c_{\alpha} X^{\alpha} \in k[X]$ be symmetric, where $k$ is a field and $X = (x_1, \ldots, x_n)$.

Assume that $\mathbb{N}^n$ is equipped with the degree-lexicographic order and that $\text{Deg}(f) = \beta = (\beta_1, \ldots, \beta_n)$.

(i) Prove that if $c_{\alpha} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ occurs with nonzero coefficient $c_{\alpha}$, then every monomial $x_{\sigma 1}^{\alpha_1} \cdots x_{\sigma n}^{\alpha_n}$ also occurs in $f(X)$ with nonzero coefficient, where $\sigma \in S_n$.

(ii) Prove that $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n$.

(iii) If $e_1, \ldots, e_n$ are the elementary symmetric polynomials, prove that

$$\mathrm{Deg}(e_i) = (1, \ldots, 1, 0, \ldots, 0),$$

where there are $i$ 1's.

(iv) Let $(\gamma_1, \ldots, \gamma_n) = (\beta_1 - \beta_2, \beta_2 - \beta_3, \ldots, \beta_{n-1} - \beta_n, \beta_n)$. If $g(x_1, \ldots, x_n) = x_1^{\gamma_1} \cdots x_n^{\gamma_n}$, prove that $g(e_1, \ldots, e_n)$ is symmetric and $\mathrm{Deg}(g) = \beta$.

(v) ***Fundamental Theorem of Symmetric Polynomials.*** Prove that if $k$ is a field, then every symmetric polynomial $f(X) \in k[X]$ is a *polynomial* in the elementary symmetric functions $e_1, \ldots, e_n$. (Compare with Theorem 4.37.)

**Hint.** Prove that $h(X) = f(X) - c_\beta g(e_1, \ldots, e_n)$ is symmetric and $\mathrm{Deg}(h) < \beta$.

***Page 411*** line -5 of text Replace sentence as follows

Conversely, assume that every $f \in I$ has remainder 0 mod $G_\sigma$ but that $\{g_1, \ldots, g_m\}$ is not a Gröbner basis of $I = (g_1, \ldots, g_m)$.

***Page 416*** line 4 Left side should be $\mathrm{Deg}(X^{\delta - \mu(j)} a_{ji} g_i)$

***Page 419*** Replace Proposition 6.139 as follows:

**Proposition 6.139**. *Let $k$ be a field and let $k[X] = k[x_1, \ldots, x_n]$ have a monomial order for which $x_1 \succ x_2 \succ \cdots \succ x_n$ (for example, the lexicographic order) and, for fixed $p > 1$, let $Y = x_p, \ldots, x_n$. If $I \subseteq k[X]$ has a Gröbner basis $G = \{g_1, \ldots, g_m\}$, then $G \cap I_Y$ is a Gröbner basis for the elimination ideal $I_Y = I \cap k[x_p, \ldots, x_n]$.*

*Proof.* Recall that $\{g_1, \ldots, g_m\}$ being a Gröbner basis of $I = (g_1, \ldots, g_m)$ means that for each nonzero $f \in I$, there is $g_i$ with $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$. Let $f(x_p, \ldots, x_n) \in I_Y$ be nonzero. Since $I_Y \subseteq I$, there is some $g_i(X)$ with $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$; hence, $\mathrm{LT}(g_i)$ involves only the "later" variables $x_p, \ldots, x_n$. Let $\mathrm{Deg}(\mathrm{LT}(g_i)) = \beta$. If $g_i$ has a term $c_\alpha X^\alpha$ involving "early" variables $x_i$ with $i < p$, then $\alpha \succ \beta$, because $x_1 \succ \cdots \succ x_p \succ \cdots \succ x_n$. This is a contradiction, for $\beta$, the Degree of the leading term of $g_i$, is greater than the Degree of any other term of $g_i$. It now follows that $g_i \in k[x_p, \ldots, x_n]$. Exercise 6.92 on page 422 now shows that $G \cap k[x_p, \ldots, x_n]$ is a Gröbner basis for $I_Y = I \cap k[x_p, \ldots, x_n]$. •

***Page 421***, Exercise 6.88 Change "$x^y - y$" to "$x^2 - y$"

***Page 422*** Add a new exercise

**6.92** Let $I$ be an ideal in $k[X]$, where $k$ is a field and $k[X]$ has a monomial order. Prove that if a set of polynomials $\{g_1, \ldots, g_m\} \subseteq I$ has the property that, for each nonzero $f \in I$, there is some $g_i$ with $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$, then $I = (g_1, \ldots, g_m)$. Conclude, in the definition of Gröbner basis, that one need not assume that $I$ is generated by $g_1, \ldots, g_m$.

***Page 425***, lines 5, 6 Should read:

Note that the composite of $R$-homomorphisms is an $R$-homomorphism and, if $f$ is an $R$-isomorphism, then its inverse function $f^{-1}$ is also an $R$-isomorphism.

***Page 435*** Add the following after the proof of Proposition 7.19

See Exercise 7.79 on page 519 for the generalization of this proposition for infinitely many submodules.

***Page 437*** Replace lines -17 through -7 by

The converse of the last proposition is not true. Let $A = \langle a \rangle$, $B = \langle b \rangle$, and $C = \langle c \rangle$ be cyclic groups of orders 2, 4, and 2, respectively. If $i\colon A \to B$ is defined by $i(a) = 2b$ and $p\colon B \to C$ is defined by $p(b) = c$, then $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ is an exact sequence which is not split: $\operatorname{im} i = \langle 2b \rangle$ is not even a pure subgroup of $B$. By Exercise 7.12 on page 440, for any abelian group $M$, there is an exact sequence

$$0 \to A \xrightarrow{i'} B \sqcup M \xrightarrow{p'} C \sqcup M \to 0,$$

where $i'(a) = (2b, 0)$ and $p'(b, m) = (c, m)$, and this sequence does not split either. If we choose $M = \mathbb{I}_4[x] \sqcup \mathbb{I}_2[x]$ (the direct summands are the polynomial rings over $\mathbb{I}_4$ and $\mathbb{I}_2$, respectively), then $A \sqcup (C \sqcup M) \cong B \sqcup M$. (For readers who are familiar with infinite direct sums, which we introduce later in this chapter, $M$ is the direct sum of infinitely many copies of $\mathbb{I}_4 \sqcup \mathbb{I}_2$.)

***Page 440***, Exercise 7.3 Change "ker $f \subseteq K$" to "$K \subseteq \ker f$"

***Page 444***, line -4 Should read: "is an ***equivalence*** (or an ***isomorphism***) if there"

***Page 445***, lines -9, -8 Change each occurrence of "$\varphi$" to "$\rho$"

***Page 446***, line -6 Replace "(the intersection of two abstract sets is not defined)" by

(if two sets are not given as subsets, then their intersection may not be what one expects: for example, if $\mathbb{Q}$ is defined as all equivalence classes of ordered pairs $(m, n)$ of integers with $n \neq 0$, then $\mathbb{Z} \cap \mathbb{Q} = \varnothing$).

***Page 446***, line $-3$ Replace "$A' \cap B'$" by "$A' \cup B'$"

***Page 446***, line $-1$ Change "subset $\operatorname{arr}(u, v)$" to "set $\operatorname{arr}(u, v)$"

***Page 447***, line -6 Should read: "Exercise 7.21 on page 458."

***Page 448***, line -6 Should read:

*coproducts of $A$ and $B$, should they exist, are equivalent.*

***Page 452*** The displayed equations at the bottom should read:

$$\begin{aligned} \psi((a_i)) &= \psi\Big(\sum_i \alpha_i(a_i)\Big) \\ &= \sum_i \psi\alpha_i(a_i) = \sum_i f_i(a_i). \end{aligned}$$

***Page 453***, line 17 Should read: "$\theta\colon x \mapsto (f_i(x))$"

***Page 454*** In both diagrams, change "$X$" to "$A$"

***Page 456*** line -1 Change "$\theta\colon X \to D$" to "$\theta\colon D \to X$"

***Page 457*** Change the first sentence of Example 7.39(i):

(i) If $B$ and $C$ are subsets of a set $A$, then there are inclusion maps $i\colon B \cap C \to B$ and $j\colon B \cap C \to B$.

***Page 457***, line -4 Change "$f\colon B \to A$" to "$f\colon A \to B$"

***Page 459*** Combine parts (i) and (ii) of Exercise 7.29; add new part

(ii) If $\Omega$ is a terminal object in a category $\mathcal{C}$, prove, for any $G \in \mathrm{obj}(\mathcal{C})$, that the projections $\lambda\colon G \sqcap \Omega \to G$ and $\rho\colon \Omega \sqcap G \to G$ are equivalences.

***Page 461*** After top diagram, insert:

where $\lambda$ and $\rho$ are the equivalences in Exercise 7.29(ii).

***Page 461*** pp, many places Change "Obj($\mathcal{C}$)" to "obj($\mathcal{C}$)"

***Page 465***, line 3. Should read: sums to products

***Page 465***, line 8. Should read: $f^*(g+h) = (g+h)f$

***Page 470***, line 12 Change "$g$" to "$h$" (two times)

***Page 471***, line -1 Change "$g\colon X \to M$" to "$g\colon F \to M$"

***Page 472***, line 7 Change "$\theta\colon F \to W$" to "$\theta\colon F \to M$"

***Page 472***, line -4 Change "$v_1, \ldots, v_n$" to "$\{v_i : i \in I\}$"

***Page 472***, line -3 Change "$\varphi(v_1), \ldots, \varphi(v_n)$" to "$\{\varphi(v_i) : i \in I\}$"

***Page 474***, line 7 Change "$g\colon F \to B$" to "$g\colon F \to A$"

***Page 476***, Replace $i$ in diagram by $j$

***Page 476***, line -2 Change "$\mathbb{Z}$-module" to "$\mathbb{I}_6$-module"

***Page 483***, line -5 Change "$= g_0((r - f')b)$" to "$= g_0((r - r')b)$"

***Page 486***, line -2 Exercise 7.42 occurs prematurely, for inverse limits have not yet been defined. Move this Exercise to page 519, and call it Exercise 7.78.

***Page 486*** (new) **7.42** Prove that a group $G \in \mathrm{obj}(\mathbf{Groups})$ is a projective object if and only if $G$ is a free group. (It is proved, in Exercise 10.3 on page 793, that the only injective object in **Groups** is $\{1\}$.)

***Page 488*** Replace Exercise 7.54 as follows.

**7.54** Prove that an $R$-module $E$ is injective if and only if, for every ideal $I$ in $R$, every short exact sequence $0 \to E \to B \to I \to 0$ splits.

***Page 489*** Redo the whole page, as follows.

**Definition.** A category $\mathcal{C}$ is a $\star$-category if there is a commutative and associative binary operation $\star$: $\mathrm{obj}(\mathcal{C}) \times \mathrm{obj}(\mathcal{C}) \to \mathrm{obj}(\mathcal{C})$; that is,

(i) if $A \cong A'$ and $B \cong B'$, where $A, A', B, B' \in \mathrm{obj}(\mathcal{C})$, then $A \star B \cong A' \star B'$;

(ii) there is an equivalence $A \star B \cong B \star A$ for all $A, B \in \mathrm{obj}(\mathcal{C})$;

(iii) there is an equivalence $A \star (B \star C) \cong (A \star B) \star C$ for all $A, B, C \in \mathrm{obj}(\mathcal{C})$.

Any category having finite products or finite coproducts is a $\star$-category.

**Definition.** If $\mathcal{C}$ is a $\star$-category, define $|\mathrm{obj}(\mathcal{C})|$ to be the class of all isomorphism classes $|A|$ of objects in $\mathcal{C}$, where $|A| = \{B \in \mathrm{obj}(\mathcal{C}) : B \cong A\}$. If $\mathcal{F}(\mathcal{C})$ is the free abelian group with basis[15] $|\mathrm{obj}(\mathcal{C})|$ and $\mathcal{R}$ is the subgroup of $\mathcal{F}(\mathcal{C})$ generated by all elements of the form

$$|A \star B| - |A| - |B| \quad \text{where } A, B \in \mathrm{obj}(\mathcal{C}),$$

then the ***Grothendieck group*** $K_0(\mathcal{C})$ is the abelian group

$$K_0(\mathcal{C}) = \mathcal{F}(\mathcal{C})/\mathcal{R}.$$

(A characterization of $K_0(\mathcal{C})$ as a solution to a universal mapping problem is given in Exercise 7.58 on page 498.) For any object $A$ in $\mathcal{C}$, we denote the coset $|A| + \mathcal{R}$ by $[A]$.

We remark that the Grothendieck group $K_0(\mathcal{C})$ can be defined more precisely: $\mathcal{C}$ should be a *symmetric monoidal category* (see Mac Lane, *Categories for the Working Mathematician*, pages 157–161).

**Proposition 7.77** *Let $\mathcal{C}$ be a $\star$-category.*

(i) *If $x \in K_0(\mathcal{C})$, then $x = [A] - [B]$ for $A, B \in \mathrm{obj}(\mathcal{C})$.*

(ii) *If $A, B \in \mathrm{obj}(\mathcal{C})$, then $[A] = [B]$ in $K_0(\mathcal{C})$ if and only if there exists $C \in \mathrm{obj}(\mathcal{C})$ with $A \star C \cong B \star C$.*

*Proof.* (i) Since $K_0(\mathcal{C})$ is generated by $|\mathrm{obj}(\mathcal{C})|$, we may write

$$x = \sum_{i=1}^{r} [A_i] - \sum_{j=1}^{s} [B_j],$$

(we allow objects $A_i$ and $B_j$ to be repeated). If we now define $A = A_1 \star \cdots \star A_r$, then

$$[A] = [A_1 \star \cdots \star A_r] = \sum_i [A_i].$$

Similarly, define $B = B_1 \star \cdots \star B_s$. It is now clear that $x = [A] - [B]$.

[15] There is a minor set-theoretic problem here, for a basis of a free abelian group must be a set and not a proper class. This problem is usually avoided by assuming that $\mathcal{C}$ is a ***small category***; that is, the class $\mathrm{obj}(\mathcal{C})$ is a set.

***Page 490***, line 16 Delete "and $[A \star C] = [B \star C]$."

***Page 491***, line -3 Change "category with product" to "$\star$-category"

***Page 492***, line 4 Change "$r : K_0(R) \to \mathbb{Z}$" to "$r : \text{obj}(\mathbf{Pr}(R)) \to \mathbb{Z}$"

***Page 492***, line 14 Change "$K_0(\mathcal{C})$" to "$K'(\mathcal{C})$"

***Page 494***, line 16 Should read:

in a category $\mathcal{C}$ of modules is called a ***composition series***

***Page 496***, line 4 Change "$C'' \oplus \text{jh}(B)$" to "$C'' \oplus \text{jh}(B_1)$"

***Page 498*** In Exercise 7.58, assume also that $f(A) = f(B)$ whenever $A \cong B$

***Page 500*** In Example(vi), state that $\mathcal{N}$ is a partially ordered set under reverse inclusion

***Page 500***, line $-7$ Change "$f_j \psi_i^j$" to "$\psi_i^j f_j$"

***Page 501***, lines 7 and 10 Change "$f_j \psi_i^j$" to "$\psi_i^j f_j$"

***Page 502***, lines -5, -4 Change "$m \leq n$" to "$m \geq n$"

***Page 505*** In defintion, change "$\alpha_i : \varinjlim M_i \to M_i$" to "$\alpha_i : M_i \to \varinjlim M_i$"

***Page 506***, line 7 Change "$\alpha_i : m_i \mapsto m_i + S$" to "$\alpha_i : m_i \mapsto \lambda_i(m_i) + S$"

***Page 507***, line 7 Change "$1 \preceq 3$ and $2 \preceq 3$" to "$1 \preceq 2$ and $1 \preceq 3$"

***Page 511***, line 10, Add "where $C(U)$ is an abelian group under pointwise multiplication."

***Page 513***, line $-7$ Replace "then their module categories are equivalent." with

"then equivalence of their module categories implies $R \cong S$."

***Page 515***, line 5 Change "$(F, G)$" to "$(G, F)$"

***Page 517*** Add a sentence just before Exercises.

There is a necessary and sufficient condition, called the ***adjoint functor theorem***, that a functor be half of an adjoint pair; see Mac Lane, *Categories for the Working Mathematician*, page 117.

***Page 518***, line 15 Add a phrase:

form a set; that is, $\mathcal{C}$ and $\mathcal{D}$ are small categories. We

***Page 519*** Add new exercises.

**7.78** Prove that if $T : {}_R\mathbf{Mod} \to \mathbf{Ab}$ is an additive left exact functor preserving products, then $T$ preserves inverse limits.

**7.79** Generalize Proposition 7.19 to allow infinitely many summands. Let $\{S_i : i \in I\}$ be a family of submodules of an $R$-module $M$, where $R$ is a commutative ring. If $M = \langle \bigcup_{i \in I} S_i \rangle$, then the following conditions are equivalent.

(i) $M = \sum_{i \in I} S_i$.

(ii) Every $a \in M$ has a unique expression of the form $a = s_{i_1} + \cdots + s_{i_n}$, where $s_{i_j} \in S_{i_j}$.

(iii) For each $i \in I$,

$$S_i \cap \left\langle \bigcup_{j \neq i} S_j \right\rangle = \{0\}.$$