Errata and Typographical Errors

p. 17, lines 3-4. \( N \) is the smallest positive integer having \ldots Note, in particular, that \( N \) cannot be prime; now, suppose \ldots

p. 18, Exercise 3. \( \gcd(0, m) = |m| \).

p. 18, Exercise 13. \( \mu = |ab| \text{ and } |ab|/d \).

p. 21, line 4. Delete “)”.

p. 24, line 8. Delete the second “p.”

p. 35, Exercise 38. Using \( e = 101 \), check that \( d = 317 \). In the first line of the table, 1663 should be 1633 \ldots Using the same \( N \) and \( e = 1601 \), \ldots

p. 39, line 14. \ldots \( a^{-1}(ab) = a^{-1} \cdot 0 = 0 \ldots \)

p. 47, line 10. Given \( n \in \mathbb{Z} \), exactly one of the statements

\[
 n \in \mathbb{Z}^+, \ n = 0, \ \text{or} \ -n \in \mathbb{Z}^+
\]

is true. (This is called the trichotomy principle.)

line 15. \( \mathbb{Z}^+ \) should be \( \mathbb{Z}^+ \).

line 21. Given \( x \in F \), exactly one of the statements

\[
 x \in F^+, \ x = 0, \ \text{or} \ -x \in F^+
\]

is true.

p. 66, Exercise 14. This is correct when \( v \geq 0 \). What’s the answer when \( v < 0 \)?

p. 66, Exercise 17. Delete the first \( dx \).

p. 91, lines 1-4. \( p_1(x), \ldots, p_m(x) \) should be distinct irreducible polynomials. And \( \deg(r_j(x)) < \deg(p_j(x)^{\nu_j}) \) for \( j = 1, \ldots, m \).

p. 92, Exercise 9. Parts a. and b. are much harder than I thought when I wrote the problem. Even deciding if there are any irreducible elements of \( \mathbb{Z}_6[x] \) seems quite difficult.

p. 96, proof of Theorem 2.1. The penultimate sentence of the first paragraph should read: Thus whenever \( |z| \geq R, |f(z)| \geq |z|^n(1 - \frac{1}{2^n}) \geq R^n/2 \). At the end of the second paragraph, it should therefore be noted that \( z_o \) cannot lie on the boundary circle; this is needed to complete the contradiction at the end of the proof.

p. 116, line 3. \( (ya) \) should be \( (ya^{-1}) \) at the end of the line.

p. 117, Example 3, last line. \( \langle 2 \rangle = \langle 4 \rangle \subset \mathbb{Z}_6, \text{ and } 4 = 2 \cdot 2, \) so 4 is a multiple of 2 by a zero-divisor. On the other hand, 4 = -2, so 4 is also a multiple of 2 by a unit! In fact, in \( \mathbb{Z}_n \) it can be shown that \( \langle a \rangle = \langle b \rangle \iff a = sb \) for some unit \( s \). (N.B. One can construct a commutative ring \( R \) having elements \( a, b \) satisfying \( \langle a \rangle = \langle b \rangle \) and yet \( a = sb \) for no unit \( s \! \))
Proposition 2.2 of Chapter 3.

Exercise 16. A few symbols didn’t print here:

a. Given an ideal $J \subset S$, define

$$J = \{ a \in R : \phi(a) \in J \} \subset R.$$  

(This is usually denoted by $\phi^{-1}(J)$.) Prove that $J$ is an ideal.

b. Given an ideal $I \subset R$, define

$$J = \{ \phi(a) : a \in I \} \subset S.$$  

...Prove that $J$ is an ideal, provided $\phi$ maps onto $S$.

p. 128, last line: $\overline{3}$ should be 3.

p. 130, line 3 of the proof of Theorem 2.4. $\text{ev}_\alpha$ maps $F[x]$ onto $F[\alpha]$ and has ....

p. 132, line 5 of the proof of Corollary 2.6. The only polynomial $f(x) \in \mathbb{Q}[x]$ having $c$ as a root ... 

p. 133, Remark and Corollary 2.8. In the displayed statement marked with ($\ast$), we must assume that $\alpha \notin \mathbb{Q}$. In the application, we should point out that $\alpha \notin \mathbb{Q}$ (e.g., by applying the result of Exercise 2.2.11a).

p. 138, Exercise 28a. We must assume $p \neq 0$.

p. 143, line 8. $\psi(a + bi) = a + 3b \pmod{5}$.

p. 163, line 4. for some nonnegative integer $r$ ...

p. 184, lines 9–10. ... in $\mathbb{Z}_p^\times$ there is only one.

p. 194, lines 3–4. That is, the conjugate of $F = F_1$ (which is the flip fixing vertex 1) by $R$ is $F_2$ (which is the flip fixing vertex 2).

p. 258, line 8 of Proof of Theorem 5.8. $k(aH) \subset aH$.

p. 260, Exercise 18. Assume also that if $\alpha = 1$, then $m > 1$.

p. 265, last line “... extending $\phi (\ldots)$ and carrying $\alpha$ to $\alpha'$.”

p. 266, line 10. “If $\tilde{\phi}(p(\alpha)) = 0, ...$”

Proof of Proposition 6.4. Assume $K \neq F$.


p. 269, line 8. “splits in $K$.”

p. 272, line 15. $-\omega$ should be $\overline{\omega}$.

p. 275, line 8. $t$ should be $\ell$.

p. 277, Exercise 5. $\phi \psi^2$ should be $\psi \phi^2$.

p. 287, line −8. $|x_1 y_2 - x_2 y_2|$ should be $|x_1 y_2 - x_2 y_1|$.

p. 302, line 1. $\{ \infty \}$ should be $\mathbb{P}^1_\alpha$.

p. 304, last line. The coordinates of $B$ and $C$ are reversed.

p. 308, Figure 11. $\alpha, \beta, \gamma$ should be $\beta, \gamma$, and $\alpha$, respectively.
p. 310–11. \( t' = g(t) = \frac{-d+et}{a+bt} \), which makes the matrix 
\[
\begin{bmatrix}
  a & b \\
  -d & -e
\end{bmatrix}
\]
and \( g^{-1}(t) = \frac{-d+at}{e+bt} \).

p. 316, Exercise 18. This is false with the definitions provided. Indeed, we should really say that six points are in general position provided no three are collinear and they do not all lie on a conic. Then Exercise 18 becomes a triviality.

p. 319, line 6. \( x_1, \ldots, x_5 \in \mathbb{R}^3 \).

p. 324, line 4. \( v_2 = \frac{1}{3\sqrt{2}}(1, -4, 1) \).

p. 324, line -5. \( y_i = \sqrt{|\lambda_i|} x_i \).

p. 325, line 11. \( z_i = \sqrt{|\lambda_i|} y_i \).

p. 342, Exercise 20. A few symbols didn’t print here:

…Associate to the line \( PQ \) the point \( A = [a_{01}, a_{02}, a_{03}, a_{12}, a_{13}, a_{23}] \in \mathbb{P}^5 \).

a. Prove that \( A \) is a well-defined point in \( \mathbb{P}^5 \) determined only by the line. (…the point \( A \in \mathbb{P}^5 \) doesn’t change. …\( a'_{ij} = p'_i q'_j - p'_j q'_i \), we have \( A' = A \in \mathbb{P}^5 \).)

b. Show that \( A \) satisfies the (homogeneous) quadratic equation ...

c. Given two lines \( \ell \) and \( m \), let \( A \) and \( B \) be the corresponding points in \( \mathbb{P}^5 \). …

p. 361, line 15. “two” should be “four.”

p. 363, Exercise 6. The reference should be to Lemma 5.7.

p. 367, Exercise 30b,c. The factors of \( \frac{1}{2} \) should be 2’s.

p. 371, line 6. \( Q \) should be \( \mathbb{Q} \).

p. 378, Exercise 5. \( h = g \circ f \); interchange \( f \) and \( g \) in parts a., b., c.

p. 387, Figure 1. The labels \( P \) and \( P^{-1} \) should be interchanged.

p. 401, Exercise 1a. …prove \( \lambda^n \) is an eigenvalue of \( T^n \) ….