Exercises supplementing those in J. Rotman, *A first course in Abstract Algebra*, 2nd Ed.

Exercise ‘‘**1.1.0**’’: Mark the following true or false.

☐ (a) Given statements $S(n)$, one for each integer $n \geq 1$, if $S(n)$ is true then $S(n+1)$ is true.

☐ (b) Given statements $S(n)$, one for each integer $n \geq 1$, if $S(1), \ldots, S(n-1)$ are true, then $S(n)$ is true.

☐ (c) Every nonempty set of positive integers has a least member.

☐ (d) Every nonempty set of negative integers has a greatest member.

☐ (e) For every positive integer n, the Fibonacci number F_n is an integer.

Answers: (a) F. (b) F. (c) T. (d) T. (e) T.

Exercise ‘‘**1.1.1**’’: Show that for every natural number i, the Fibonacci number F_i is even if and only if i is divisible by 3. (Suggestion: Use the second form of induction, dividing your proof into cases according to whether i has the form $3n$, $3n+1$, or $3n+2$.)

Exercise ‘‘**1.1.2**’’: (a) Find integers a and b such that for all $i \geq 1$, $F_{i+2} = a F_i + b F_{i-1}$, and prove that equation.

(b) Find integers a' and b' such that for all $i \geq 1$, $F_{i+3} = a' F_i + b' F_{i-1}$, and prove that equation.

(c) Generalizing the above result, show that for every positive integer m there exist integers a_m and b_m such that for all $i \geq 1$, $F_{i+m} = a_m F_i + b_m F_{i-1}$, and prove that equation. Can you find exact formulas for a_m and b_m as functions of m?

Exercise ‘‘**1.1.3**’’: (a) Find integers a and b such that for all $i \geq 2$, $F_{i+2} = a F_i + b F_{i-2}$, and prove that equation.

(b) Find integers a' and b' such that for all $i \geq 3$, $F_{i+3} = a' F_i + b' F_{i-3}$, and prove that equation.

(c) Generalizing the above result, show that for every positive integer m there exist integers a_m and b_m such that for all $i \geq m$, $F_{i+m} = a_m F_i + b_m F_{i-m}$, and prove that equation. Can you find exact formulas for a_m and b_m as functions of m?

Exercise ‘‘**1.1.4**’’: Show that in the power series expansion of $(1-x-x^2)^{-1}$, the coefficients are Fibonacci numbers. Which Fibonacci number gives the coefficient of x^n?

Exercise ‘‘**1.1.5**’’: This exercise concerns positive integers a, b, c that satisfy

$$a+b = c \quad\text{and}\quad ac-b^2 = \pm 1.$$

(i) Show that for all integers $n > 1$, a solution to the above pair of equations is given by $a = F_{n-1}$, $b = F_n$, $c = F_{n+1}$.

(ii) Show, conversely, that if a, b, c are positive integers that satisfy the two equations displayed above, then there exists an integer $n > 1$ such that $a = F_{n-1}$, $b = F_n$, and $c = F_{n+1}$.

(Suggestion: Show that if a, b, c satisfy the above equations, so do $b-a$, a, b; then use one of the two forms of induction.)

Exercise ‘‘**1.1.6**’’: Can we continue the sequence of Fibonacci numbers to the left, getting values for $\ldots, F_{-3}, F_{-2}, F_{-1}$ that ‘‘mesh with’’ the known values of F_0, F_1, $F_2, \ldots$?

To answer this question, assume values F_n exist for all $n < 0$ which, together with the known values for $n \geq 0$, make the equation $F_n = F_{n-1} + F_{n-2}$ hold for all n, and figure out what a few such values must be. From these values, guess a formula relating F_{-n} and F_n, and finally, prove that if this formula is taken as the definition of Fibonacci numbers with negative subscripts, the equation $F_n = F_{n-1} + F_{n-2}$ does indeed hold for all n, and so does the equation proved in Theorem 1.13.

Exercise ‘‘**1.2.0**’’: Mark the following true or false.

☐ (a) If n is a positive integer, then $(x+1)^n$ expands to a polynomial with n terms.

☐ (b) If $S = \{1, \ldots, 20\}$ and $T = \{11, \ldots, 30\}$, then the number of 5-subsets of S is equal to the number of 5-subsets of T.

☐ (c) $\{i, -i\}$ is the set of all 4th roots of unity in $\mathbb{C}$.

☐ (d) $i^{999} = -i$.

Answers: (a) F. (b) T. (c) F. (d) T.

Exercise ‘‘**1.2.1**’’: Show that for every positive integer n, $F_{n+1} = \Sigma \binom{n-i}{i}$, where the sum is over all values of i such that $0 \le i \le n-i$. (Suggestion for getting started: Draw a few levels of Pascal’s triangle, and mark which terms the above formula says add up to F_3, which to F_4, to F_5, etc..)

Exercise ‘‘**1.2.2**’’: Let n be an integer > 1. Show that if x and y are positive real numbers such that $y < x \tan \pi/2n$, then the complex number $(x+iy)^n$ has positive real and imaginary parts. (For an imaginary number $z = a + ib$, one calls a the real part of z and b the imaginary part.)

Exercise ‘‘**1.3.0**’’: Mark the following true or false.

☐ (a) $6\,|\,2$. ☐ (b) $2\,|\,6$. ☐ (c) $6\,|\,0$. ☐ (d) $0\,|\,6$.

☐ (e) For every integer n, $(n, n+1) = 1$.

☐ (f) For every integer n, $(n, n+2) = 2$.

☐ (g) If a, b and c are integers such that $a\,|\,bc$, then $a\,|\,b$ or $a\,|\,c$.

☐ (h) If a and b are positive integers, then $a\,|\,b$ if and only if the last digit, d_0, in the base-a expansion of b is 0.

Answers: (a) F. (b) T. (c) T. (d) F. (e) T. (f) F. (g) F. (h) T.

Exercise ‘‘**1.4.0**’’: Mark the following true or false.

☐ (a) $|2^{19} - 3^{12}| \le 1/2$.

☐ (b) If $r = p_1^{g_1} \ldots p_n^{g_n}$ where $p_1, \ldots p_n$ are distinct primes, and $g_1, \ldots, g_n$ are integers, then r is an integer if and only if $g_1, \ldots, g_n$ are all nonnegative.

Answers: (a) F. (b) T.

Exercise ‘‘**1.4.1**’’: Suppose a and b are relatively prime integers.

(i) Show using Proposition 1.44 that if a and b are relatively prime, then so are a^2 and b^2.

(ii) Show the same result without using the Fundamental Theorem of Arithmetic. (Suggestion: Take an equation $sa + tb = 1$ and cube both sides.)

(iii) Same task as in part (ii) for a^m and b^n, where m and n are any positive integers.

Exercise ‘‘**1.4.2**’’: Suppose a, b and n are positive integers, and p is a prime. Show that if ab is divisible by p^n but a is not divisible by p^n then b is divisible by p.

Exercise ‘‘**1.5.0**’’: Mark the following true or false.

☐ (a) If a and m are integers with $m > 0$, then there is some $i \in \{0, \ldots, m-1\}$ such that $a \equiv i \pmod{m}$.

☐ (b) If a, b, c and m are integers such that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

☐ (c) If a, b, c and m are integers with $m > 0$, then $(a+b)^m \equiv a^m + b^m \pmod{m}$.

☐ (d) For p is a prime and a an integer, $a^p \equiv p \pmod{a}$.

☐ (e) For p is a prime and a an integer, $a^p \equiv a \pmod{p}$.

☐ (f) There exists an integer n such that the last five digits of $7n$ (written in base 10) are 00001.

☐ (g) There exists an integer n such that $n \equiv 1 \bmod 100$ and $n \equiv 4 \bmod 1000$.

☐ (h) There exists an integer n such that $n \equiv 1 \bmod 100$ and $n \equiv 4 \bmod 1001$.

☐ (i) If m and n are positive integers such that $m \equiv n \bmod 4$ and $m \equiv n \bmod 25$, then the last two digits of m (in base 10) are the same as the last two digits of n.

Answers: (a) T. (b) T. (c) F. (d) F. (e) T. (f) T. (g) F. (h) T. (i) T.

Exercise ‘‘**1.5.1**’’: If a, b, c and m are integers, show that $a + c \equiv b + c \pmod{m}$ if and only if $a \equiv b \pmod{m}$.

Exercise ‘‘**1.5.2**’’: If a, b, d and m are integers, show that $da \equiv db \pmod{dm}$ if and only if $a \equiv b \pmod{m}$.

Exercise ‘‘**1.5.3**’’: If a, b, c and m are integers with $a \equiv b \pmod{m}$, does it follow that $c^a \equiv c^b \pmod{m}$? If so, prove it; if not, give a counterexample.

Exercise ‘‘**1.5.4**’’: (i) Show that for every integer $a \geq 2$, $\binom{a}{2} = a(a-1)/2$.

Now suppose a and b are integers ≥ 2, and n an integer such that $a \equiv b \bmod n$.

(ii) Show that if n is odd, then $\binom{a}{2} \equiv \binom{b}{2} \bmod n$.

(iii) Show by example that for $n = 2$, the conclusion of (ii) need not hold.

(iv) For larger i, what can you say about conditions on n and i under which $a \equiv b \bmod n$ will or will not imply $\binom{a}{i} \equiv \binom{b}{i} \bmod n$?

Exercise ‘‘**1.5.5**’’: (i) Suppose m and n are positive integers, a is any integer, and p is a prime. Show that if $m \equiv n \bmod p{-}1$, then $a^m \equiv a^n \bmod p$.

(ii) Show by example that the statement of (i) becomes false if ‘‘positive integers’’ is weakened to ‘‘nonnegative integers’’.

(iii) Show by example that the statement of (i) also becomes false if the assumption $m \equiv n \bmod p{-}1$ is changed to $m \equiv n \bmod p$.

Exercise ‘‘**1.5.6**’’: Suppose n is a positive integer, and a and b arbitrary integers. The Chinese Remainder Theorem guarantees that there will exist a solution to the system of congruences $x \equiv a \bmod n$, $x \equiv b \bmod n{+}1$. Find an explicit formula for such a solution. (You may do this using the method of proof of the Chinese Remainder Theorem, or by any other technique. If it is not obvious from the way you obtain your answer that it satisfies the given congruences, then you should show this.)

Exercise ‘‘**1.5.7**’’: (i) The form of the Chinese Remainder Theorem given in the text only concerns systems of congruences in which the moduli m and n are relatively prime. Prove the following more general form of the Chinese Remainder Theorem:

Let m and n be any positive integers, and let a and b be any integers. Then the system of congruences

$$x \equiv a \bmod n \qquad x \equiv b \bmod m$$

has a solution if and only if $a \equiv b \bmod (m, n)$.

Suggestion: Show that a solution to this system, if it exists, must have the form $a + ny$ for some integer y. Write out the condition that y must satisfy to make $a + ny$ a solution to the above system. Then show that there exists a y satisfying that condition if and only if $a \equiv b \bmod (m, n)$.

(ii) Deduce the case of the Chinese Remainder Theorem given in the text from the result of (i).

Exercise ‘‘**1.5.8**’’: (Cf. Rotman’s Exercise 1.69, p.72, and footnote.) What is the remainder on dividing $10^{10^{100}}$ by 7?

Exercise ''**2.1.0**'': Mark the following true or false.

☐ (a) If $S \subset T \subset U$, then $S \subset U$.

☐ (b) If $S \subset T$, then $T \subset S$.

☐ (c) For any set S, $S \subset S$.

☐ (d) If $f : X \to Y$ is a function, then $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

☐ (e) A function $f : X \to Y$ with the property that $\forall\, y \in Y\ \exists\, x \in X$ such that $f(x) = y$ is called surjective.

☐ (f) A function that is both injective and surjective is called bijective.

☐ (g) Any functions $f : X \to Y$ and $g : Y \to Z$ have a composite function $f \circ g : X \to Z$.

Answers: (a) T. (b) F. (c) T. (d) F. (e) T. (f) T. (g) F.

Exercise ''**2.1.1**'': Suppose $f : X \to Y$ and $g : Y \to Z$ are functions.

(i) Show that if $g \circ f$ is injective, then f is injective.

(ii) Show by example that if $g \circ f$ is injective, g may not be injective.

(iii) Show that if $g \circ f$ is surjective, then g is surjective.

(iv) Show by example that if $g \circ f$ is surjective, f may not be surjective.

Exercise ''**2.2.0**'': Mark the following true or false.

☐ (a) The symmetric group on n letters is a set of n elements.

☐ (b) If $\alpha, \beta \in S_n$, then $\alpha \circ \beta \in S_n$.

☐ (c) For $\alpha, \beta \in S_n$, $\alpha\beta$ is an abbreviation for $\alpha \circ \beta$.

☐ (d) If $\alpha, \beta \in S_n$, then $\alpha\beta = \beta\alpha$.

☐ (e) If $\alpha, \beta \in S_n$ are disjoint, then $\alpha\beta = \beta\alpha$.

☐ (f) If σ and τ are r-cycles in S_n, then $\sigma\tau$ is an r-cycle.

☐ (g) If σ is an r-cycle in S_n and τ is any element of S_n, then $\tau\sigma\tau^{-1}$ is an r-cycle.

☐ (h) If σ is an r-cycle in S_n then σ^{-1} is an r-cycle.

☐ (i) Every transposition is an even permutation.

☐ (j) Every transposition is an odd permutation.

☐ (k) If an element $\sigma \in S_n$ can be written as a product of 3 transpositions, then σ cannot be written as a product of 4 transpositions.

☐ (l) If an element $\sigma \in S_n$ can be written as a product of 3 transpositions, then σ cannot be written as a product of 5 transpositions.

Answers: (a) F. (b) T. (c) T. (d) F. (e) T. (f) F. (g) T. (h) T. (i) F. (j) T. (k) T. (l) F.

Exercise ''**2.2.1**'': Let n and d be positive integers, and let $\sigma \in S_n$.

(i) If d is an odd positive integer, show that σ^d is an even permutation if and only if σ is an even permutation, and is an odd permutation if and only if σ is an odd permutation.

(ii) If d is an even positive integer, give a rule determining whether σ^d is even or odd.

Exercise ''**2.2.2**'': Suppose σ is an r-cycle in S_n, where $r > 1$.

(i) Show that if r is odd, then σ^2 is also an r-cycle.

(ii) Show that if r is even, then σ^2 is not an r-cycle, and determine the form of its expression as a product of disjoint cycles. (You will need to consider separately the cases $r = 2$ and $r > 2$.)

(iii) Can you generalize the above results to a criterion for σ^m to be an r-cycle, for a given integer m, in terms of the properties of m and r, and a description of the cycle decomposition of σ^m when it is not an r-cycle?

Exercise ''**2.3.0**'': Mark the following true or false.

☐ (a) Every operation on a set is associative.

☐ (b) Every group has an identity element.

☐ (c) Every group is abelian.

☐ (d) If α, β and γ are permutations of a set X, and if $\alpha\beta = \gamma\beta$, then $\alpha = \gamma$.

☐ (e) The set of all positive real numbers forms a group under the operation of multiplication.

☐ (f) The set of all nonnegative real numbers forms a group under the operation of multiplication.

☐ (g) The set of all nonnegative real numbers forms a group under the operation of addition.

☐ (h) The set of all real numbers forms a group under the operation of addition.

☐ (i) The set of all real numbers forms a group under the operation of subtraction.

☐ (j) The set of all integers forms a group under the operation of addition.

☐ (k) The set of all positive integers forms a group under the operation of multiplication.

In the remaining parts of this question, G denotes a group, written multiplicatively.

☐ (l) For all $a, b, c \in G$, $(a\,b\,c)^{-1} = c^{-1}b^{-1}a^{-1}$.

☐ (m) For all $a, b \in G$, $a\,b\,(b\,a)^{-1} = 1$.

☐ (n) For all $a, b \in G$ and all positive integers n, $(a\,b)^n = a^n b^n$.

☐ (o) If $a \in G$ and n is a positive integer such that $a^n = 1$, then n is the order of a.

☐ (p) If $a \in G$ has finite order n, then $a^n = 1$.

☐ (q) If $a \in G$ has finite order, then for any integer n, $a^n = 1$ if and only if n is a multiple of the order of a.

☐ (r) An element $a \in G$ has infinite order if and only if $a^n = 1$ holds for infinitely many integers n.

☐ (s) If G is an infinite group, then it has elements of infinite order.

☐ (t) If two motions α and β are symmetries of a geometric figure X, then the composite motion $\alpha\beta$ is also a symmetry of X.

☐ (u) If X and Y are subsets of the plane, and α and β are motions such that α is a symmetry of X and β is a symmetry of Y, then $\alpha\beta$ is a symmetry of $X \cup Y$.

☐ (v) If X and Y are subsets of the plane, and α is a motion which is a symmetry of both X and Y, then α is also a symmetry of $X \cap Y$.

Answers: (a) F. (b) T. (c) F. (d) T. (e) T. (f) F. (g) F. (h) T. (i) F. (j) T. (k) F. (l) T. (m) F. (n) F. (o) F. (p) T. (q) T. (r) F. (s) F. (t) T. (u) F. (v) T.

Exercise ''**2.3.1**'': Let n be a positive integer. Show that the n-element set $\{0, 1, \ldots, n-1\}$ forms a group under the operation $+_n$, defined by letting $a +_n b$ be the remainder on dividing $a + b$ by n.

(Note: For every a and b in $\{0, 1, \ldots, n-1\}$, the element $a +_n b$ will equal either $a + b$ or $a + b - n$, depending on whether or not $a + b < n$. The hard way of proving the associative law $(a +_n b) +_n c = a +_n (b +_n c)$ is to work through lots of cases, according to whether each sum in the calculation is $< n$ or $\geq n$. The nice way is to verify that $a +_n b$ is the unique element of $\{0, 1, \ldots, n-1\}$ that is congruent mod n to $a + b$, and use basic facts about congruence mod n.)

Exercise ''**2.3.2**'': Let $* : \mathbb{Z} \times \mathbb{Z} \to Z$ be the operation defined by $m * n = m + n + 1$. Let G denote the set $\mathbb{Z}$ equipped with the operation $*$. Determine whether G is a group. (Of course, a question like this requires that you prove the correctness of the answer you give.)

Exercise ‘‘**2.3.3**’’: Let a and b be elements of a finite group G, which commute with each other, i.e., satisfy $ab = ba$.

(i) Show that if a has order m and b has order n, then the order of ab is a divisor of the least common multiple of m and n.

(ii) Find an example of the situation of (i) in which the order of ab equals the least common multiple of m and n, and an example in which it does not.

(iii) Show that, in general, the orders of a, of b and of ab are three integers such that every pair of them has the same l.c.m.. Verify that the examples you gave in (ii) have this property.

Exercise ‘‘**2.3.4**’’: Let $n > 1$, let $\sigma = (1\ 2)(3\ 4)\ldots(2n\text{–}1\ \ 2n)$, and let $\tau = (2\ 3)(4\ 5)\ldots(2n\text{–}2\ \ 2n\text{–}1)$ in the symmetric group S_{2n}.

(i) Find the cycle decomposition of $\sigma\tau$.

(ii) Find the orders of σ, τ and $\sigma\tau$. Does this example contradict what you proved in ‘‘Exercise 2.3.3(i)’’?

Exercise ‘‘**2.3.5**’’: Consider the operation of *subtraction* on $\mathbb{Z}$. Since it is not associative, what Rotman (p.12) might call the various ‘‘ultimate values’’ obtained from a sequence of four integers, a_1, a_2, a_3, a_4 under subtraction are not, in general, all equal. Write out all the formulas obtained by inserting parentheses and minus-signs among those symbols, and show that *two* of them are, in general, equal.

Exercise ‘‘**2.4.0**’’: Mark the following true or false. Here G is always a group.

☐ (a) A subgroup of a subgroup of G is a subgroup of G.

☐ (b) A subset H of G is a subgroup if there exists an operation on H which makes it a group.

☐ (c) G is a subgroup of G.

☐ (d) G is a proper subgroup of G.

☐ (e) The empty set $\varnothing$ is a subgroup of G.

☐ (f) If m is any integer dividing the order of G, then G has an element of order m.

☐ (g) Every subgroup of S_n has order dividing $n!$.

☐ (h) The intersection of any two subgroups of G is a subgroup of G.

☐ (i) If H is a subgroup of G, the intersection of any two cosets of H is a coset of H.

☐ (j) If H is a subgroup of G, the union of any two cosets of H is a coset of H.

Answers: (a) T. (b) F. (c) T. (d) F. (e) F. (f) F. (g) T. (h) T. (i) F. (j) F.

Exercise ‘‘**2.5.0**’’: Mark the following true or false.

☐ (a) If G and H are groups which are both written additively, then a homomorphism $G \to H$ means a function $f: G \to H$ satisfying $f(x+y) = f(x) + f(y)$ for all $x, y \in G$.

☐ (b) A map $f: \mathbb{R} \to \mathbb{R}^{\times}$ is a homomorphism if and only if $f(x+y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$.

☐ (c) The inclusion map of any subgroup in a group is a homomorphism.

☐ (d) The inclusion map of $\mathbb{Z}$ in $\mathbb{R}$ is an isomorphism.

☐ (e) The subgroup $\{0\}$ of $\mathbb{R}$ is isomorphic to the subgroup $\{1\}$ of $\mathbb{R}^{\times}$.

☐ (f) If p and q are prime numbers, then every group of order p is isomorphic to every group of order q.

☐ (g) Any two finite groups of the same order are isomorphic.

☐ (h) In S_3, the subgroup $\langle (1\ 2) \rangle$ is normal.

☐ (i) In S_3, the subgroup $\langle (1\ 2\ 3) \rangle$ is normal.

☐ (j) If G is a group, $Z(G) = G$ if and only if G is abelian.

☐ (k) If G is a group, $Z(Z(G)) = Z(G)$.

☐ (l) In S_{100}, the elements $(1\ 8\ 99)$ and $(7\ 6\ 5)$ are conjugate.

Answers: (a) T. (b) F. (c) T. (d) F. (e) T. (f) F. (g) F. (h) F. (i) T. (j) T. (k) T. (l) T.

Exercise ‘‘**2.5.1**’’: Let $(G, \cdot)$ be a group, K a set, and $f: G \to K$ a bijection (a one-to-one and onto map). Show that there is a binary operation $*$ on K such that $(K, *)$ forms a group and f is an isomorphism. (Hint: The group operation $\cdot$ of G and the condition that f be an isomorphism determine precisely how $*$ must operate on K.)

Exercise ‘‘**2.6.0**’’: Mark the following true or false.

☐ (a) For every integer $m > 1$, $\mathbb{Z}_m$ is an infinite set.

☐ (b) If $[a] = [b]$ in $\mathbb{Z}_m$, then $a = b$ in $\mathbb{Z}$.

☐ (c) If $a = b$ in $\mathbb{Z}$, then $[a] = [b]$ in $\mathbb{Z}_m$.

☐ (d) The rule $f([a]) = a$ defines a function $\mathbb{Z}_m \to \mathbb{Z}$.

☐ (e) If a, a', b, b', m are integers with $m > 1$, such that $[a] = [a']$ and $[b] = [b']$ in $\mathbb{Z}_m$, then $[a + b] = [a' + b']$ in $\mathbb{Z}_m$.

☐ (f) If a, a', b, b', m are integers with $m > 1$, such that $[a] = [a']$ and $[b] = [b']$ in $\mathbb{Z}_m$, then $[a\,b] = [a'\,b']$ in $\mathbb{Z}_m$.

☐ (g) If K is a normal subgroup of a group G, then there exists a homomorphism $G \to G/K$ having kernel K.

☐ (h) If K is a normal subgroup of a group G, then every homomorphism $G \to G/K$ has kernel K.

☐ (i) If $f: G \to H$ is a group homomorphism, and K is its kernel, then $f(G) \cong G/K$.

☐ (j) If $f: G \to H$ is a surjective group homomorphism, and K is its kernel, then $H \cong G/K$.

☐ (k) If G and H are groups, and K a normal subgroup of G such that $H \cong G/K$, then there exists a surjective group homomorphism $f: G \to H$ with kernel K.

☐ (l) If G is a group of order m and H is a group of order n, then $G \times H$ is a group of order $m\,n$.

☐ (m) If G and H are abelian groups, then $G \times H$ is an abelian group.

☐ (n) If G and H are cyclic groups, then $G \times H$ is an cyclic group.

Answers: (a) F. (b) F. (c) T. (d) F. (e) T. (f) T. (g) T. (h) F. (i) T. (j) T. (k) T. (l) T. (m) T. (n) F.

Exercise ‘‘**2.6.1**’’: Within the group $\mathrm{Aff}(1, \mathbb{R})$, let us use the notation $f_{a,b}$ for elements, introduced in the correction to Exercise 2.87 above, and let $A = f_{1,1}$ and $B = f_{-1,0}$. (This exercise will revolve around these two elements, so I suggest you write out on scratch-paper the formulas for A and B, and make pictures for yourself of what they do to points of the line $\mathbb{R}$, before proceeding further.)

(i) Show that $BA = A^{-1}B$.

(ii) Let G be the subset $\langle A \rangle \cup B\langle A \rangle$ of $\mathrm{Aff}(1, \mathbb{R})$. Show that G is a subgroup of $\mathrm{Aff}(1, \mathbb{R})$.

(iii) Show that in S_4, if we write $\alpha = (1\ 2\ 3\ 4)$ and $\beta = (1\ 3)$, then $\beta\alpha = \alpha^{-1}\beta$.

(iv) Show that there is a homomorphism $f: G \to S_4$ such that $f(A) = \alpha$ and $f(B) = \beta$, for α and β defined as above.

(v) Show that the image of the homomorphism defined in (iv) is the subgroup $\langle \alpha, \beta \rangle$.

(vi) Show that the kernel of the homomorphism defined in (iv) is the subgroup $\langle A^4 \rangle$.

(vii) Deduce that $\langle A^4 \rangle \lhd G$, and that the subgroup $\langle \alpha, \beta \rangle$ of S_4 is isomorphic to $G/\langle A^4 \rangle$.

Exercise ‘‘**2.6.2**’’: This exercise will develop a simpler proof of Proposition 2.65. Hence, in doing the parts of this exercise, you may use results proved in the book before that proposition, but not that proposition itself. As in that proposition, let us assume throughout this exericise that:

G is a finite abelian group, of order n, such that for every prime p dividing n, G has a unique cyclic subgroup of order p.

Now for every positive integer r, let us define $\mu_r : G \to G$ by $\mu_r(x) = x^r$.

(i) Show that for every positive integer r, μ_r is a homomorphism.

(ii) Show that for p a prime dividing n, $|\mathrm{ker}(\mu_p)| = p$.

(iii) Show that $\mathrm{ker}(\mu_n) = G$.

Our plan will be to show G cyclic by showing $\mathrm{ker}(\mu_r)$ cyclic for larger and larger r, leading to the conclusion that $\mathrm{ker}(\mu_n) = G$ is cyclic. So let r be any positive integer and p any prime dividing n. In the next four steps we will show that if $\mathrm{ker}(\mu_r)$ is cyclic, then so is $\mathrm{ker}(\mu_{pr})$.

(iv) Show that the homomorphism μ_p, when restricted to $\mathrm{ker}(\mu_{pr})$, has image a subgroup of $\mathrm{ker}(\mu_r)$, and that the kernel of this restricted homomorphism still has order p.

(v) Deduce that in the situation of (iv), either $\mathrm{ker}(\mu_{pr}) = \mathrm{ker}(\mu_r)$, or $[\mathrm{ker}(\mu_{pr}) : \mathrm{ker}(\mu_r)] = p$; and that the latter happens if and only if μ_p maps $\mathrm{ker}(\mu_{pr})$ *onto* $\mathrm{ker}(\mu_r)$.

(Hint: Look at inclusion relations among the groups $\mathrm{ker}(\mu_{pr})$, $\mu_p(\mathrm{ker}(\mu_{pr}))$ and $\mathrm{ker}(\mu_r)$, and arithmetic relations among their orders.)

Obviously, if $\mathrm{ker}(\mu_{pr}) = \mathrm{ker}(\mu_r)$ then if $\mathrm{ker}(\mu_r)$ is cyclic, so is $\mathrm{ker}(\mu_{pr})$, as desired. In the alternative situation, we have two cases:

(vi) Suppose $\mathrm{ker}(\mu_r)$ is cyclic, say of order s, and s is not divisible by p. Show that the product of any generator of $\mathrm{ker}(\mu_r)$ and any generator of $\mathrm{ker}(\mu_p)$ is a generator of $\mathrm{ker}(\mu_{pr})$, so the latter group is cyclic. (Hint: Proposition 2.63.)

(vii) Suppose $\mathrm{ker}(\mu_r)$ is cyclic, say of order s, and s is divisible by p, and that μ_p maps $\mathrm{ker}(\mu_{pr})$ *onto* $\mathrm{ker}(\mu_r)$. Show that any element $x \in \mathrm{ker}(\mu_{pr})$ which is mapped by μ_p to a generator of $\mathrm{ker}(\mu_r)$ has order ps. Deduce that $\mathrm{ker}(\mu_{pr})$ is cyclic.

(viii) Combining the results proved above, show by induction that for every $r|n$, $\mathrm{ker}(\mu_r)$ is cyclic, and conclude that G is cyclic.

Exercise ‘‘**2.6.3**’’: This exercise concerns subgroups of $\mathbb{Z} \times \mathbb{Z}$.

(a) Let $D \subseteq \mathbb{Z} \times \mathbb{Z}$ denote the set $\{(a, a) \mid a \in \mathbb{Z}\}$. (This is called the *diagonal* subset of $\mathbb{Z} \times \mathbb{Z}$, for a reason which can be seen by graphing it in the plane.) Show that D is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

(b) For any positive integer n, let $C_n \subseteq \mathbb{Z} \times \mathbb{Z}$ denote $\{(a, b) \mid a \equiv b \bmod n\}$. Show that C_n is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

(c) Let $G \subseteq \mathbb{Z} \times \mathbb{Z}$ denote $\{(a, b) \mid a \geq b\}$. Show that G is not a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

(d) Show that every subgroup of $\mathbb{Z} \times \mathbb{Z}$ which properly contains the subgroup D of part (a) above has the form C_n as in part (b) above for some positive integer n.

Exercise ‘‘**2.6.4**’’: (a) Let $C_2 \subseteq \mathbb{Z} \times \mathbb{Z}$ be the subgroup defined in ‘‘Exercise 2.6.3(b)’’ above, with $n = 2$. Show that there is an isomorphism $f : \mathbb{Z} \times \mathbb{Z} \to C_2$ which takes $(1, 0)$ to $(2, 0)$, and $(0,1)$ to $(1,1)$. (You need to determine what f does to the general element of $\mathbb{Z} \times \mathbb{Z}$, and prove that the map you have defined is an isomorphism.)

(b) Show, in fact, that for every positive integer n the subgroup $C_n \subseteq \mathbb{Z} \times \mathbb{Z}$ of ‘‘Exercise 2.6.3(b)’’ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$.

Exercise ‘‘**2.6.5**’’: A positive integer m is called *square-free* if it is not divisible by the square of any integer > 1. Show that any finite abelian group of square-free order is cyclic. Deduce that if m is a square-free positive integer, then all abelian group of order m are isomorphic.

Exercise ‘‘**2.7.0**’’: Mark the following true or false.

☐ (a) Every group G is isomorphic to the symmetric group S_G.

☐ (b) If r is an integer such that there exists a nonabelian group of order r, then S_r has a nonabelian subgroup of order r.

☐ (c) Every group of order 4 is abelian.

☐ (d) Every group of order 6 is abelian.

☐ (e) If a group G acts on a set X, then X is a group.

☐ (f) If a group G acts on a set X, and $x \in X$, then the orbit of x is a subset of X.

☐ (g) If a group G acts on a set X, and $x, y \in X$, then there is some $g \in G$ such that $y = gx$.

☐ (h) If a group G acts on a set X, and if $g, h \in G$, $x \in X$ satisfy $gx = hx$, then $g = h$.

☐ (i) For g an element of a finite group G, the number of conjugates of g in G is a divisor of $|G|$.

☐ (j) If a group G has a subgroup of order 100, then it has an element of order 5.

☐ (k) If a group G has a subgroup of order 100, then it has an element of order 4.

☐ (l) Every group of order 5^8 has a subgroup of order 5^6.

☐ (m) If G is a simple group of order p^n, where p is a prime and n a positive integer, then $n = 1$.

☐ (n) The alternating group A_4 is simple.

☐ (o) The alternating group A_5 is simple.

☐ (p) The symmetric group S_6 is simple.

Answers: (a) F. (b) T. (c) T. (d) F. (e) F. (f) T. (g) F. (h) F. (i) T. (j) T. (k) F. (l) T. (m) T. (n) F. (o) T. (p) F.

Exercise ‘‘**2.8.0**’’: Mark the following true or false.

☐ (a) If a group G acts on a set X, and $x, y \in X$ are elements lying in the same orbit, then G_x and G_y are isomorphic.

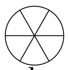
☐ (b) If a group G acts on a set X, and $x, y \in X$ are elements of X such that G_x and G_y are isomorphic, then x and y are in the same orbit.

☐ (c) If a finite group G acts on a finite set X so that no element of G other than 1 fixes any element of X, then the number of orbits of the action is $|X| / |G|$.

Answers: (a) T. (b) F. (c) T.

Exercise ‘‘**2.8.1**’’: Suppose a group G acts on a set X. Show that $\{\sigma \in G \mid \forall\, x \in X,\ \sigma x = x\}$ is a normal subgroup of G.

Exercise ‘‘**2.8.2**’’: (This is Rotman’s Exercise 2.109, rewritten so as not to assume the unclearly stated material that we skipped.)

Consider a disk, divided into 6 equal sectors by lines through the center: . Suppose you have q colors of paint, and want to paint each sector of the disk with one solid color (where colors may be repeated). Suppose, moreover, that you consider two colorings to be essentially the same if one of them can be obtained from the other by rotating through a multiple of 60°, and you want to know how many essentially different colorings are possible.

(i) Translate this question into one about the number of orbits of an action of a certain group (which you should describe clearly) on a certain set (which you should describe clearly).

(ii) Show that this number is $\frac{1}{6}(2q+2q^2+q^3+q^6)$.

Exercise ‘‘**2.8.3**’’: (i) Suppose a finite group G acts on a set X in such a way that there is only one orbit, and suppose that every element of G fixes at least one element of X. Show that $|X| = 1$.

(ii) Find an example of a finite group G acting on a set X with more than one orbit, in such a way that every element of G fixes at least one element of X, but every orbit has more than one element.

(iii) Find an example of an infinite group G acting on an infinite set X such a way that there is only one orbit, and every element of G fixes at least one element of X.

(iv) Show that if in part (iii) ‘‘an infinite set X’’ is changed to ‘‘a finite set X with more than one element’’ (but G still assumed infinite), then no example exists.

Exercise ‘‘**3.1.0**’’: Mark the following true or false.

☐ (a) Every commutative ring is a set of numbers.

☐ (b) For every element a of a commutative ring, $(-1)\,a = -a$.

☐ (c) For every real number u, the subset of $\mathbb{R}$ consisting of all elements $a+bu$ with $a,b\in\mathbb{Q}$ forms a subring of $\mathbb{R}$.

☐ (d) If R is a commutative ring, and A is an additive subgroup of R which contains 1, then A is a subring of R.

☐ (e) If R is a commutative ring, and A is a subring of R, then A is an additive subgroup of R and contains 1.

☐ (f) Any subring of a domain is a domain.

☐ (g) There are infinitely many positive integers m such that $\mathbb{Z}_m$ is a domain.

☐ (h) If R is an infinite commutative ring, then $U(R)$ is an infinite group.

☐ (i) If R is any commutative ring, then $U(R)$ is a subgroup of the additive group of all elements of R.

☐ (j) If R is a ring and S a subring of R, then $U(S)$ is a subgroup of $U(R)$.

☐ (k) If R is a ring and S a subring of R, then $U(S) = U(R)\cap S$.

☐ (l) The symbols $\mathbb{Q}^{\times}$ (introduced on p.118) and $U(\mathbb{Q})$ (this reading) denote the same group.

Answers: (a) F. (b) T. (c) F. (d) F. (e) T. (f) T. (g) T. (h) F. (i) F. (j) T. (k) F. (l) T.

Exercise ‘‘**3.2.0**’’: Mark the following true or false.

☐ (a) Every field is a domain.

☐ (b) Every domain contains a field.

☐ (c) Every subring of a field is a field.

☐ (d) Every field has infinitely many elements.

☐ (e) If for real numbers x and y, we write $x\#y$ to mean $|x-y| < 1$, then $\#$ is an equivalence relation on $\mathbb{R}$.

☐ (f) If G is a group, and for $g,h\in G$ we write $g \sim h$ to mean that g is conjugate to h in G, then $\sim$ is an equivalence relation on G.

☐ (g) Let X be the set of all ordered pairs of real numbers. If for (a,b), $(c,d)\in X$ we define $(a,b)\equiv(c,d)$ to mean $a + b^2 = c + d^2$, then $\equiv$ is an equivalence relation on X.

☐ (h) Let X be the set of all ordered pairs of real numbers. If for (a,b), $(c,d)\in X$ we define $(a,b)\equiv(c,d)$ to mean $a + c^2 = b + d^2$, then $\equiv$ is an equivalence relation on X.

☐ (i) If $\equiv$ is an equivalence relation on a set X, and two equivalence classes $[x]$ and $[y]$ have an element in common, then $x = y$.

☐ (j) If $\equiv$ is an equivalence relation on a set X, and two equivalence classes $[x]$ and $[y]$ have an element in common, then $[x] = [y]$.

☐ (k) If $\equiv$ is an equivalence relation on a set X, then $X = \bigcup_{x \in X} [x]$.

☐ (l) If $\equiv$ is an equivalence relation on a set X, and we choose one member from each equivalence class, and write the set of chosen elements as $\{x_i : i \in I\}$, then $X = \bigcup_{i \in I} [x_i]$.

☐ (m) Every domain is contained in a field.

☐ (n) For every domain A, there is a unique field F containing A.

Answers: (a) T. (b) F. (c) F. (d) F. (e) F. (f) T. (g) T. (h) F. (i) F. (j) T. (k) T. (l) T. (m) T. (n) F.

Exercise ‘‘**3.2.1**’’: Although 2×2 matrices over a field do not form a commutative ring, you have seen the rules for adding and multiplying them; these are the addition and multiplication you will use in this problem.

Let R denote the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ over $\mathbb{R}$, and let A denote the set of all 2×2 matrices M over $\mathbb{R}$ which satisfy $RM = MR$.

(i) Show that $A = \{aI + bR : a, b \in \mathbb{R}\}$.

(ii) Show that A is closed under the operations of matrix addition and multiplication, and that under these operations, A forms a field. (In particular, this means you must prove that the operation of matrix multiplication is commutative on A.) You may take as a known fact that multiplication of matrices is an associative operation.

Exercise ‘‘**3.3.0**’’: Mark the following true or false.

☐ (a) If A is a domain, then $A[x]$ is a domain.

☐ (b) If A is not a domain, then $A[x]$ is not a domain.

☐ (c) If F is a field, then $F[x]$ is a field.

☐ (d) In the construction of rings of polynomials used by Rotman, the polynomial $x^3 - x + 2$ is represented as $(2, -1, 0, 1, 0, 0, 0, \ldots)$.

☐ (e) If A is a domain and $f, g \in A[x] - \{0\}$, then $\deg(fg) = \deg(f) + \deg(g)$.

☐ (f) If A is a domain and $f, g \in A[x] - \{0\}$, then $\deg(f + g) = \deg(f) \deg(g)$.

☐ (g) If A is a domain and $f, g \in A[x] - \{0\}$ have the same degree n, then $\deg(f + g) = n$.

☐ (h) If F is a field, then $F[x] = F(x)$

Answers: (a) T. (b) T. (c) F. (d) T. (e) T. (f) F. (g) F. (h) F.

Exercise ‘‘**3.4.0**’’: Mark the following true or false.

☐ (a) If R and S are commutative rings, and $f: R \to S$ is a ring homomorphism, then f is also a homomorphism from the additive group R to the additive group S.

☐ (b) If R and S are commutative rings, and $f: R \to S$ is a homomorphism from the additive group R to the additive group S, then f is also a ring homomorphism.

☐ (c) If R and S are commutative rings, and $f: R \to S$ is a ring homomorphism, and if f is also an isomorphism from the additive group R to the additive group S, then it is a ring isomorphism.

☐ (d) If R and S are commutative rings which are isomorphic to one another, and $f: R \to S$ is a ring homomorphism, then f is an isomorphism.

☐ (e) If $f : R \to S$ is a homomorphism of commutative rings, then $\ker(f)$ is an ideal of R.

☐ (f) If I and J are ideals of the commutative ring R, then $I \cap J$ is also an ideal of R.

☐ (g) If I and J are ideals of the commutative ring R, then $I \cup J$ is also an ideal of R.

☐ (h) If R is a commutative ring, and $a \in R$, then $\{ra : r \in R\}$ is an ideal of R.

☐ (i) If $f : R \to S$ is a homomorphism of commutative rings, and I is an ideal of R, then $f(I)$ is an ideal of S.

☐ (j) If $f : R \to S$ is a homomorphism of commutative rings, and I is an ideal of S, then $f^{-1}(I)$ is an ideal of R.

Answers: (a) T. (b) F. (c) T. (d) F. (e) T. (f) T. (g) F. (h) T. (i) F. (j) T.

Exercise ‘‘**3.4.1**’’: Show that Exercise 3.46(ii) remains true if the word ‘‘isomorphism’’ is replaced by ‘‘injective homomorphism’’, but becomes false if that word is simply replaced by ‘‘homomorphism’’.

Exercise ‘‘**3.4.2**’’: This exercise uses the concept of direct product of rings, so it should be done after Exercise 3.49.

In doing this exercise, recall that Rotman has defined congruence $\bmod n$ for any nonnegative integer n, including $n = 0$, though he noted that usually one is only interested in $n \geq 2$. In this problem, however, all nonnegative integer values of n will be of interest. (We see that $a \equiv b \bmod 0$ holds if and only if $a = b$, while $a \equiv b \bmod 1$ holds for all a and b.)

(i) For each nonnegative integer n, let $C_n \subseteq \mathbb{Z} \times \mathbb{Z}$ denote $\{(a, b) : a \equiv b \bmod n\}$. Show that C_n is a subring of $\mathbb{Z} \times \mathbb{Z}$.

(ii) Suppose R is a subring of $\mathbb{Z} \times \mathbb{Z}$. Show that $R \supseteq C_0$. Show moreover that if this inclusion is proper (i.e., if $R \neq C_0$) then R contains the pair $(n, 0)$ for some positive integer n, and that if n is the least positive integer with this property, then $R = C_n$.

(iii) Conclude that the subrings of $\mathbb{Z} \times \mathbb{Z}$ are precisely the subsets C_n for nonnegative integers n.

Exercise ‘‘**3.4.3**’’: Part (ii) below shows that subrings of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ are not so easy to describe.

(i) Given any three nonnegative integers n, n', n'', let $C_{n,n',n''} = \{(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} : a \equiv b \bmod n,$ $a \equiv c \bmod n',\ b \equiv c \bmod n''\}$. Show that $C_{n,n',n''}$ is a subring of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

(ii) Show that there are subrings of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ not of the form described in (i).

Exercise ‘‘**3.4.4**’’: (i) Show that if S is a subring of a commutative ring R, then the inclusion map $R \to S$ is a ring homomorphism. Deduce that there exist ring homomorphisms $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$.

(ii) Show that there do not exist any ring homomorphisms $\mathbb{C} \to \mathbb{R} \to \mathbb{Q} \to \mathbb{Z}$ (i.e., that none of those three arrows can represent any ring homomorphism; I show them together only for brevity).

(iii) Show that there does not exist any ring homomorphism $\mathbb{Q} \to \mathbb{Z}_p$ for any prime p.

(iv) If R and S are commutative rings, show that the following conditions are equivalent: (a) There exists a ring homomorphism $R \to S$, (b) There exists a ring homomorphism $R \to S[x]$, (c) There exists a ring homomorphism $R[x] \to S$.

Exercise ‘‘**3.5.0**’’: Mark the following true or false.

☐ (a) If $a(x),\ b(x) \in \mathbb{Q}[x]$ with $b(x) \neq 0$, then there exist $c(x),\ d(x) \in \mathbb{Q}[x]$ such that $a(x) = b(x)\,c(x) + d(x)$, and $d(x)$ is either 0 or of degree $< \deg(b(x))$.

☐ (b) If $f(x),\ g(x) \in \mathbb{Z}[x]$ with $f(x) \neq 0$, then there exist $q(x),\ r(x) \in \mathbb{Z}[x]$ such that $g(x) = q(x)\,f(x) + r(x)$, and $r(x)$ is either 0 or of degree $< \deg(f(x))$.

☐ (c) For every quadratic polynomial $s(x) \in \mathbb{C}[x]$, there exist $u, v \in \mathbb{C}$ and $q(x) \in \mathbb{C}[x]$ such that $(x+1)^{1000} = s(x)\,q(x) + ux + v$.

☐ (d) If k is a field, and $f(x),\ g(x) \in k[x]$, and if for all $a \in k$ one has $f(a) = g(a)$, then $f(x) = g(x)$.

☐ (e) If k is a field, then $k[x]$ is a PID.

☐ (f) If k is a field, then in $k[x]$, every nonzero constant polynomial is an irreducible.

☐ (g) If k is a field, and $f(x)$ is a polynomial of positive degree which has no root in k, then $f(x)$ is irreducible in $k[x]$.

☐ (h) If $f(x)/g(x) \in k(x)$, then $f(x)$ and $g(x)$ are relatively prime in $k[x]$.

☐ (i) $\mathbb{Z}$ is a euclidean ring.

☐ (j) $\mathbb{R}[x]$ is a euclidean ring.

☐ (k) There exists an integer m such that $m^2 \equiv -1 \bmod 89$.

Answers: (a) T. (b) F. (c) T. (d) F. (e) T. (f) F. (g) F. (h) F. (i) T. (j) T. (k) T.

Exercise ‘‘**3.5.1**’’: (i) Factor each of the integers 5 and 13 as a product of two nonunits in $\mathbb{Z}[i]$. Obtain from these a factorization of 65 as a product of four nonunits in $\mathbb{Z}[i]$.

(ii) Find two different ways of grouping these factors so as to obtain a factorization of 65 as a product $\alpha\bar{\alpha}$ of two conjugate factors. Use these to get two different expressions of 65 as a sum of two squares.

Exercise ‘‘**3.5.2**’’: (i) Find necessary and sufficient conditions on integers m and n for the element $m+ni \in \mathbb{Z}[i]$ to belong to the ideal $\langle 1+2i \rangle$ of $\mathbb{Z}[i]$. (Your conditions should constitute a simple arithmetic test that one can apply to any two integers m and n to determine whether $m+ni \in \langle 1+2i \rangle$.)

(ii) Apply the above conditions to determine the ideal $\langle 1+2i \rangle \cap \mathbb{Z}$ of $\mathbb{Z}$.

(iii) Investigate the analogous questions for a general principal ideal $\langle m+ni \rangle$ of $\mathbb{Z}[i]$. (Suggestion: first study the case where m and n are relatively prime, then the case where they have given g.c.d., say g.c.d.$(m,n) = d$.)

Exercise ‘‘**3.5.3**’’: Let F be a field, and n a positive integer.

(i) Suppose $a(x),\ b(x),\ c(x) \in F[x]$, with $b(x)$ and $c(x)$ nonzero. Let $q(x)$ and $r(x)$ be the quotient and remainder on dividing $a(x)$ by $b(x)$. Show that the remainder on dividing $a(x)$ by $b(x)\,c(x)$ can be expressed in terms of $r(x)$ and the remainder on dividing $q(x)$ by $c(x)$.

(ii) For $\alpha \in F$, determine the remainder when x^n is divided by $(x-\alpha)^2$.

(iii) For distinct elements $\alpha,\ \beta \in F$, determine the remainder when x^n is divided by $(x-\alpha)(x-\beta)$.

(iv) Taking $F = \mathbb{R}$ and considering the graphs of the polynomials of part (iii) above, state in geometric terms the conditions a polynomial $r(x)$ should satisfy to be the remainder on dividing x^n by $(x-\alpha)(x-\beta)$ (i.e., the conditions of having smaller degree than $(x-\alpha)(x-\beta)$, and of differing from x^n by a multiple of that polynomial) and verify that the polynomial found in (iii) satisfies these conditions.

(v) Do the same for the polynomial found in part (ii).

Exercise ‘‘**3.6.0**’’: Mark the following true or false.

☐ (a) Every element of $\mathbb{Z}[x]$ is a product of a constant in $\mathbb{Z}$, and monic irreducible polynomials in $\mathbb{Z}[x]$.

☐ (b) Every element of $\mathbb{Z}[x]$ is a product of a constant in $\mathbb{Z}$ and monic irreducible polynomials in $\mathbb{Q}[x]$.

☐ (c) If a polynomial $f(x)$ over a field k can be written both as $a\,p_1(x) \ldots p_m(x)$ and as $b\,q_1(x) \ldots q_n(x)$, where a and b are constants in k, $p_1(x),\ \ldots,\ p_m(x)$ are monic irreducible polynomials, and $q_1(x),\ \ldots,\ q_n(x)$ are monic nonconstant polynomials, then $q_1(x),\ \ldots,\ q_n(x)$ are irreducible.

☐ (d) If a polynomial $f(x)$ over a field k can be written both as $a\,p_1(x)\dots p_m(x)$ and as $b\,q_1(x)\dots q_n(x)$, where a and b are constants in k, $p_1(x),\ \dots,\ p_m(x)$ are monic irreducible polynomials, and $q_1(x),\ \dots,\ q_n(x)$ are monic nonconstant polynomials, then $m \geq n$.

☐ (e) If $f(x)$ is a polynomial over a field k, and its factorization into a constant and monic irreducible polynomials in $k[x]$ is $a\,p_1(x)\dots p_m(x)$, and if k is a subfield of another field K, then $a\,p_1(x)\dots p_m(x)$ is also the factorization of $f(x)$ into a constant and monic irreducible polynomials in $K[x]$.

☐ (f) If $f(x)$ is a polynomial over a field K, and its factorization into a constant and monic irreducible polynomials in $K[x]$ is $a\,p_1(x)\dots p_m(x)$, and if all the coefficients of $f(x)$ and of the polynomials $p_i(x)$ belong to a subfield $k \subseteq K$, then $a\,p_1(x)\dots p_m(x)$ is also the factorization of $f(x)$ into a constant and monic irreducible polynomials in $k[x]$.

Answers: (a) F. (b) T. (c) F. (d) T. (e) F. (f) T.

Exercise ‘‘**3.6.1**’’: Show that for any positive integer n, the polynomial $x^n - 1$ has precisely 2^n distinct monic divisors in $\mathbb{C}[x]$. (Here we are not talking about irreducible divisors; we want to count all monic polynomials $f(x)$ such that $f(x) \mid x^n - 1$, including even the constant polynomial 1. After indicating how to describe these 2^n polynomials, you must prove from results in the reading that they are all distinct, and that no other monic polynomials divide $x^n - 1$.) In doing this exercise you may use the result of Exercise 3.74.

Exercise ‘‘**3.7.0**’’: Mark the following true or false.

☐ (a) If $f(x) = 3x^4 + ax^3 + bx^2 + cx + 7$ with $a, b, c \in \mathbb{Z}$, then the roots of $f(x)$ in $\mathbb{Q}$ (if any) lie in the set $\{\pm 1, \pm 7, \pm 1/3, \pm 7/3\}$.

☐ (b) If $f(x) = 3x^4 + ax^3 + bx^2 + cx + 7$ with $a, b, c \in \mathbb{Q}$, then the roots of $f(x)$ in $\mathbb{Q}$ (if any) lie in the set $\{\pm 1, \pm 7, \pm 1/3, \pm 7/3\}$.

☐ (c) $6x^2 + 10x + 15$ is a primitive polynomial.

☐ (d) Every primitive polynomial over $\mathbb{Z}$ is irreducible.

☐ (e) Every irreducible polynomial over $\mathbb{Z}$ is primitive.

☐ (f) Every monic polynomial over $\mathbb{Z}$ is primitive.

☐ (g) The content of $3x + 1/5$ is $3/5$.

☐ (h) The content of $3x + 6/5$ is $3/5$.

☐ (i) If $f(x) = g(x)\,h(x)$ in $\mathbb{Q}[x]$, and $f(x)$ has coefficients in $\mathbb{Z}$, then $g(x)$ and $h(x)$ have coefficients in $\mathbb{Z}$.

☐ (j) If a, b and c are integers, then $(3a+1)x^2 + (3b-1)x + (3c-1)$ is irreducible in $\mathbb{Q}[x]$.

☐ (k) For all integers n, the polynomial $x^8 + 5x^3 + 5n$ is irreducible in $\mathbb{Q}[x]$.

☐ (l) For all integers n, the polynomial $x^7 + 9x^3 + (9n+6)$ is irreducible in $\mathbb{Q}[x]$.

Answers: (a) T. (b) F. (c) T. (d) F. (e) F. (f) T. (g) F. (h) T. (i) F. (j) T. (k) F. (l) T.

Exercise ‘‘**3.7.1**’’: Let $m, n \in \mathbb{Z}$, and let $f(x) = x^4 + mx^2 + nx + 1$.

(i) Show that if $f(x)$ is reducible in $\mathbb{Z}[x]$ but does not have 1 or -1 as a root, then it has a factorization of the form $(x^2 + ax + 1)(x^2 - ax + 1)$ or $(x^2 + ax - 1)(x^2 - ax - 1)$ for some $a \in \mathbb{Z}$.

(ii) Deduce that $f(x)$ is reducible if and only if either (a) $m + n = -2$, or (b) $m - n = -2$, or (c) $n = 0$ and the integer $2 - m$ is a square, or (d) $n = 0$ and the integer $-2 - m$ is a square.

(iii) Apply the above result to show that the polynomials of Exercise 3.75, parts (vi) and (vii), are both irreducible, and likewise the polynomial $x^4 + 1$. (That last polynomial is shown in Exercise 3.86 to be reducible in $\mathbb{Z}_p[x]$ for every prime p.)

Exercise ‘‘**3.7.2**’’: Let p be a prime.

(i) Show that an action of the additive group $\mathbb{Z}_p$ on the set $\mathbb{Z}_p[x]$ is define by $[n] * f(x) = f(x+n)$.

(ii) Show that for each natural number d, the set of irreducible polynomials of degree d in $\mathbb{Z}_p[x]$ is carried into itself by the above action.

(iii) Find the orbits, under the above action, into which each of the sets of irreducible polynomials in the lists on p.275 decomposes.

Exercise ‘‘**3.8.0**’’: Mark the following true or false.

☐ (a) If I is a proper ideal of a commutative ring R, then the natural map $\pi: R \to R/I$ has kernel I.

☐ (b) If I is a proper ideal of a commutative ring R, then the natural map $\pi: R \to R/I$ is surjective.

☐ (c) If $f: R \to S$ is a homomorphism of commutative rings, and $I = \ker(f)$, then S has a subring isomorphic to R/I.

☐ (d) If I is a proper ideal of a commutative ring R, then R has a subring isomorphic to R/I.

☐ (e) If p is a prime number, then every field of characteristic p is finite.

☐ (f) Every field of characteristic 0 is infinite.

☐ (g) If $f(x)$ is an irreducible polynomial over a field k, then the factor ring $k[x]/(f(x))$ is a field.

☐ (h) If $f(x)$ is a nonconstant polynomial over a field k and if the factor ring $k[x]/(f(x))$ is a field, then $f(x)$ is irreducible.

☐ (i) If $f(x)$ is an irreducible polynomial over a field k, then every element z of the factor ring $k[x]/(f(x))$ is a root of $f(x)$.

☐ (j) If $k \subseteq K$ are fields and $z \in K$ is a root of some nonzero polynomial $p(x) \in k[x]$, then $p(x)$ is irreducible in $k[x]$.

☐ (k) If k is a field and $f(x)$ is a nonzero polynomial over k, then there exists a field K containing k as a subfield such that $f(x)$ has a root in K.

☐ (l) For every positive integer n, there exists a field with exactly 11^n elements.

☐ (m) For every positive integer n, there exists a field with exactly 10^n elements.

☐ (n) For every positive integer n, there exists a field with exactly 9^n elements.

☐ (o) There exists a field E containing $\mathbb{Z}_2$ as a subfield such that in $E[x]$, the polynomial $x^4 + x + 1$ is a product of linear factors.

☐ (p) There exists a field k such that the group $k^\times$ is isomorphic to $\mathbb{Z}_{48}$.

☐ (q) There exists a field k such that the group $k^\times$ is isomorphic to $\mathbb{Z}_{47}$.

☐ (r) There exists a field k such that the group $k^\times$ is isomorphic to V.

☐ (s) There exists a field k such that the group $k^\times$ is isomorphic to S_3.

Answers: (a) T. (b) T. (c) T. (d) F. (e) F. (f) T. (g) T. (h) T. (i) F. (j) F. (k) T. (l) T. (m) F. (n) T. (o) T. (p) T. (q) F. (r) F. (s) F.

Exercise ‘‘**3.8.1**’’: Let $k \subseteq K$ be fields, and let $z \in K$ be an element which is a root of an irreducible polynomial $p(x) \in k[x]$. Show the converse to Proposition 3.76(iii): If θ is any homomorphism $k(z) \to K$ such that $\theta(a) = a$ for all $a \in k$, then $\theta(z)$ is also a root of $p(x)$.

Exercise ‘‘**3.8.2**’’: Again let $k \subseteq K$ be fields and $z \in K$ an element which is a root of an irreducible polynomial $p(x) \in k[x]$.

(i) Show that for every polynomial $f(x) \in k[x]$, the following conditions are equivalent:

(a) $f(z) = 0$. (b) $p(x) \mid f(x)$.

(ii) Show by example that statement (i) becomes false if ‘‘$f(x) \in k[x]$’’ is changed to ‘‘$f(x) \in K[x]$’’.

Exercise ‘‘**3.8.3**’’: Let $k \subseteq K$ be fields, and let $z \in K$ be an element which is *not* a root of any nonzero polynomial in $k[x]$. Prove that $k(z)$ is isomorphic to $k(x)$ (the field of rational functions over k) by an isomorphism φ with $\varphi(x) = z$ and $\varphi(a) = a$ for all $a \in k$.

Exercise ‘‘**3.8.4**’’: Suppose K is a finite field, with exactly p^n elements. Show that every element of K is a root of the polynomial $x^{p^n} - x$. (Hint: Have you seen the $n = 1$ case of this result?) Deduce that the polynomial $x^{p^n} - x + 1$ has no roots in K.

Exercise ‘‘**3.8.5**’’: Find an isomorphism between the fields $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ and $\mathbb{Q}[x]/\langle x^2 + 4x + 2\rangle$. (Hints: Don’t expect the isomorphism to take the $[x]$ of one field to the $[x]$ of the other. Before doing this exercise, I suggest you find the roots of $x^2 + 4x + 2$ in $\mathbb{R}$, and relate them to the structure of $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.)

Exercise ‘‘**3.8.6**’’: Show that the fields $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ and $\mathbb{Q}[x]/\langle x^2 - 3\rangle$ are *not* isomorphic.

Exercise ‘‘**3.8.7**’’: (i) Show that every finite integral domain is a field.

(ii) Deduce that if R is a finite ring, then every prime ideal of R is maximal.

(iii) For n an arbitrary integer > 1, determine all prime ideals of $\mathbb{Z}_n$.

Exercise ‘‘**5.2.0**’’: Mark the following true or false.

☐ (a) If G is a finite group and p a prime, then G has at most one Sylow p-subgroup.

☐ (b) If G is a finite group and p a prime, then G has at least one Sylow p-subgroup.

☐ (c) If H is a subgroup of a group G, then every conjugate of H is also a subgroup of G.

☐ (d) If a group G acts on a set X, and x, y are elements of X belonging to the same orbit of this action, then G_x and G_y are conjugate subgroups of G.

☐ (e) If a group G acts on a set X, and x, y are elements of X such that G_x and G_y are conjugate subgroups of G, then x and y belong to the same orbit of the action of G on X.

☐ (f) If $H < G$, then $N_G(H) \lhd H$.

☐ (g) If $H < G$, then $H \lhd N_G(H)$.

☐ (h) If $H \lhd G$, then $N_G(H) = G$.

In the next five parts, the phrase ‘‘It is possible’’ means that there is no direct contradiction with the facts we have seen proved in §5.2. So in each case, you should look at the results of that section, and see whether they exclude the situation mentioned. (In fact, every possibility mentioned below that is not excluded by the results of §5.2 does occur in some group.)

☐ (i) It is possible for a group of order 400 to have exactly 6 Sylow 5-subgroups.

☐ (j) It is possible for a group of order 400 to have exactly 8 Sylow 5-subgroups.

☐ (k) It is possible for a group of order 400 to have exactly 16 Sylow 5-subgroups.

☐ (l) It is possible for a group of order 400 to have exactly 1 Sylow 5-subgroup.

☐ (m) It is possible for a Sylow 5-subgroup of a group of order 400 to have order 5.

☐ (n) A Sylow p-subgroup of a group G contains all other p-subgroups of G.

☐ (o) If G_1 and G_2 are finite groups with Sylow p-subgroups $P_1 < G_1$, $P_2 < G_2$ and if $|G_1| = |G_2|$, then $|P_1| = |P_2|$.

Answers: (a) F. (b) T. (c) T. (d) T. (e) F. (f) F. (g) T. (h) T. (i) F. (j) F. (k) T. (l) T. (m) F. (n) F. (o) T.

Exercise ‘‘**5.2.1**’’: Let G be a group.

(i) Show that if H is a subgroup of G, then H is a conjugate of itself in G.

(ii) Show that if H_1 and H_2 are subgroups of G such that H_2 is a conjugate of H_1, then H_1 is a conjugate of H_2.

(ii) Show that if H_1, H_2 and H_3 are subgroups of G such that H_2 is a conjugate of H_1 and H_3 is a conjugate of H_2, then H_3 is a conjugate of H_1.

Exercise ‘‘**5.2.2**’’: (i) Show that if x is an element of order 2 in a group G, then $N_G(\langle x\rangle) = C_G(x)$, where the right-hand side denotes the centralizer of x, defined on p.185.

(ii) Show that the result of (i) is not true for elements of arbitrary order, by letting $G = S_3$, $x = (1\ 2\ 3)$, and finding $N_G(\langle x\rangle)$ and $C_G(x)$.

Exercise ‘‘**5.2.3**’’: Suppose G is a finite group, p a prime, and P a Sylow p-subgroup of G. Show that if $P < H < G$, then P is also a Sylow p-subgroup of H.

Exercise ‘‘**6.1.0**’’: Mark the following true or false.

☐ (a) If R is a commutative ring and I is an ideal of R, and we apply the correspondence theorem for groups to the additive group R and its subgroup I, then the subgroups of R containing I which are ideals correspond to the subgroups of R/I which are ideals of that ring.

☐ (b) In the same situation, those subgroups of R containing I which are not ideals of R correspond to those subgroups of R/I which are not ideals of that ring.

☐ (c) If I is an ideal of a ring R, and $r, s\in R$ are elements such that $rs\in I$, then $r\in I$ or $s\in I$.

☐ (d) If k is a field and $(p(x))$ a nonzero prime ideal of $k[x]$, then $\deg(p(x))$ is a prime number.

☐ (e) If k is a field and $p(x)$ an irreducible polynomial over k, then $(p(x))$ is a prime ideal of $k[x]$.

☐ (f) In the ring $\mathbb{Z}$, there is exactly one prime ideal that is not a maximal ideal.

☐ (g) If R is a ring, k a field, and $f: R \to k$ a surjective homomorphism, then $\ker(f)$ is a maximal ideal of R.

☐ (h) If R is a ring, k a field, and $f: R\to k$ any homomorphism, then $\ker(f)$ is a maximal ideal of R.

☐ (i) If R is a ring, k a field, and $f : R \to k$ any homomorphism, then $\ker(f)$ is a prime ideal of R.

Answers: (a) T. (b) T. (c) F. (d) F. (e) T. (f) T. (g) T. (h) F. (i) T.

Exercise ‘‘**6.1.1**’’: Let R and I be as in Proposition 6.1, and let $J < R$, $J/I < R/I$ be ideals related by the correspondence of that proposition.

(a) Show that $R/J \cong (R/I)/(J/I)$ (isomorphism as rings).

(b) Deduce that J is prime if and only if J/I is prime, and that J is maximal if and only if J/I is maximal.

Exercise ‘‘**6.1.2**’’: Suppose R is a commutative ring, I is an ideal of R, and J, J' are two ideals of R which contain I. (We are *not* assuming $J \subseteq J'$ as in Proposition 6.1.) Show that $(J \cap J')/I = (J/I) \cap (J'/I)$.

Exercise ‘‘**6.2.0**’’: Mark the following true or false.

☐ (a) If a, b, c are elements of a domain R, and a and b are associates, then $a\,|\,c$ if and only if $b\,|\,c$.

☐ (b) If a, b, c are elements of a domain R, and a and b are associates, then $c\,|\,a$ if and only if $c \mid b$.

☐ (c) $\mathbb{Z}$ is a unique factorization domain.

☐ (d) If an element a of a unique factorization domain has two factorizations into irreducibles, $a = p_1 \dots p_m = q_1 \dots q_n$, then $m = n$, and for each i, $p_i = q_i$.

☐ (e) If an element a of a unique factorization domain has two factorizations into irreducibles, $a = p_1 \dots p_m = q_1 \dots q_n$, then $m = n$ and for each i, p_i and q_i are associates.

☐ (f) If an element a of a unique factorization domain has two factorizations into irreducibles, $a = p_1 \dots p_m = q_1 \dots q_n$, then $m = n$ and there exists $\sigma \in S_m$ such that for each i, $p_i = q_{\sigma(i)}$.

☐ (g) If an element a of a unique factorization domain has two factorizations into irreducibles, $a = p_1 \dots p_m = q_1 \dots q_n$, then $m = n$ and there exists $\sigma \in S_m$ such that for each i, p_i and $q_{\sigma(i)}$ are associates

☐ (h) If R is a PID, then there exists no infinite strictly ascending chain of ideals $I_1 < I_2 < \dots < I_n < I_{n+1} < \dots$.

☐ (i) If R is a PID, then there exists no infinite strictly descending chain of ideals $I_1 > I_2 > \dots > I_n > I_{n+1} > \dots$.

☐ (j) If R is a UFD and u is a unit of R, then u is relatively prime to every element of R.

☐ (k) If R is a PID, then $R[x]$ is a PID.

☐ (l) If R is a UFD, then $R[x]$ is a UFD.

☐ (m) If R is a PID, then $R[x]$ is a UFD.

Answers: (a) T. (b) T. (c) T. (d) F. (e) F. (f) F. (g) T. (h) T. (i) F. (j) T. (k) F. (l) T. (m) T.

Exercise ‘‘**6.2.1**’’: Prove the following result (which, as we will see in the next exercise, can be used to simplify the proof of Theorem 6.16):

Lemma 6.15½. *Let R be an integral domain and I a nonzero ideal of $R[x]$.*

(i) *If $m(x)$ is a nonzero element of least degree in I, then for every $f(x) \in I$ there exists a nonzero element $b \in R$ such that $b f(x) \in (m(x))$.*

(ii) *If, moreover, R is a UFD, and if I has the property that for nonzero $c \in R$ and $h(x) \in R[x]$, $c\,h(x) \in I \Rightarrow h(x) \in I$, then the $m(x)$ of part* (i) *can be chosen to be primitive, and in that case, $I = (m(x))$.*

(Hint: (i) is an abstraction of the trick on p.453, using the field of fractions Q of R; (ii) is an abstraction of the arguments used after that.)

Exercise ‘‘**6.2.2**’’: Suppose, as in Case (ii) of the proof of Theorem 6.16 (p.453) that R is a UFD, $p(x)$ is an irreducible element of positive degree in $R[x]$, hence primitive, and that $f(x), g(x)$ are elements of $R[x]$ such that $p(x) \mid f(x)\,g(x)$ but $p(x) \nmid f(x)$. To complete the proof of the Theorem, one needs to show that $p(x) \mid g(x)$.

Let us define $I = \{ h(x) \in R[x] : p(x) \mid f(x)\,h(x) \}$.

(i) Show that I is an ideal of $R[x]$ which contains $p(x)$ and $g(x)$ but not 1, and has the property that for nonzero $c \in R$ and $h(x) \in R[x]$, if $c\,h(x) \in I$ then $h(x) \in I$.

(ii) Deduce from Exercise ‘‘6.2.1’’ that there is a polynomial $m(x)$ of positive degree which divides both $p(x)$ and $g(x)$.

(iii) Deduce using the irreducibility of $p(x)$ that $m(x)$ is an associate of $p(x)$.

(iv) Deduce that $p(x) \mid g(x)$ (as required to complete the proof of Theorem 6.16).