Exercises supplementing those in Dummit and Foote's *Abstract Algebra*, 3rd Edition

Most of the items in this collection are exercises that I put on homework sheets when I taught Honors undergraduate Abstract Algebra in Spring 2009, supplementing those in the text. Some I included in the assignments to be handed in, but most I described as for ‘‘students interested in further interesting and/or more challenging problems’’ to think about. Many are more challenging than exercises I would give; at the other end are easy results that filled in what I felt were gaps in the text's material (e.g., the first exercise below).

I adapted a number of these exercises from my similar packet of exercises supplementing those in Beachy and Blair (though I did not take any exercises from that text).

Some of these exercises have many parts. In such cases, if I assigned some parts, I generally left out others, as either being more difficult, or adding too much length to an already long assignment.

I have given the exercises numbers indicating the relevant section of the text, and continuing the numeration where the exercises in that section leave off, except, occasionally, when I have numbered an exercise as a variant or an ‘‘additional part’’ to one in the text. The numbers of all my exercises are shown in quotation marks, to distinguish them from the exercises in the text.

These pages are accessible online as http://math.berkeley.edu/~gbergman/ug.hndts/mH113_D+F_exs.ps .

George M. Bergman
gbergman@math.berkeley.edu
June 2009

– = ≡ ≡ = –

§0.1, ‘‘**Exercise 8**’’: Show that if $\sim$ is an equivalence relation on a set A, and C is the equivalence class of an element $a \in A$ with respect to this relation, then for every $b \in C$, the set C is also the equivalence class of b with respect to $\sim$.

(This shows that the phrase ‘‘the equivalence class of a’’ can be understood as meaning ‘‘the unique equivalence class containing a’’.)

Note: Since the above exercise concerns the fundamentals of the concept of equivalence relation, you should say at each step what properties from the definition of equivalence relation you are using; likewise, you should use the definition of equivalence class in precisely the form in which it is given. Later, when we have gotten past the basics, it will be acceptable to take a lot of facts about equivalence relations and their equivalence classes for granted (such as the one you are proving in this exercise).

§0.1, ‘‘**Exercise 9**’’: Suppose A is a set, and R, S are subsets of $A \times A$. Prove that the answer to one of the following questions is positive, and show by example that the answer to the other is negative:

(i) If R and S are equivalence relations on A, must $R \cap S$ also be an equivalence relation?

(ii) If R and S are equivalence relations on A, must $R \cup S$ also be an equivalence relation?

§0.1, ‘‘**Exercise 10**’’: Let X and Y be sets, and $f: X \to Y$ a function.

(a) Show that if $\sim_Y$ is an equivalence relation on Y, and we define a relation $\sim_X$ on X by letting $x_1 \sim_X x_2$ hold for $x_1, x_2 \in X$ if and only if $f(x_1) \sim_Y f(x_2)$ holds, then $\sim_X$ is an equivalence relation on X. This is called the equivalence relation obtained by ‘‘pulling $\sim_Y$ back via f’’.

In the next four parts we will not assume an equivalence relation given on Y; rather, we shall assume an equivalence relation $\sim_X$ is given on X, and try to construct from it an equivalence relation $\sim_Y$ on Y.

This is not as easy.

(b) If f is surjective, we might try to define $\sim_Y$ by declaring that $f(x_1) \sim_Y f(x_2)$ if and only if $x_1 \sim_X x_2$. Show by example that this may fail to give a well-defined relation.

(c) Suppose instead that we define $\sim_Y$ by writing $y_1 \sim_Y y_2$ if and only if *there exist* elements $x_1, x_2 \in X$ such that $f(x_1) = y_1$, $f(x_2) = y_2$ and $x_1 \sim_X x_2$. Here there is no question of well-definedness, but show by example that even for f surjective, the relation on Y so defined may fail to be an equivalence relation.

(d) Show likewise, again with f surjective, that if one defines $\sim_Y$ by letting $y_1 \sim_Y y_2$ if and only if for *all* pairs of elements $x_1, x_2 \in X$ such that $f(x_1) = y_1$ and $f(x_2) = y_2$, one has $x_1 \sim_X x_2$, this relation may fail to be an equivalence relation.

(e) Show, however, that whether or not f is surjective, the set of equivalence relations $\sim$ on Y which satisfy $(\forall\, x_1, x_2 \in X)\ (x_1 \sim_X x_2 \Rightarrow f(x_1) \sim f(x_2))$ has a *least* member; i.e., that there is an equivalence relation, which we shall call $\sim_Y$, that satisfies the above condition, and which, as a subset of $Y \times Y$, is contained in every equivalence relation $\sim$ that satisfies that condition.

This may be called the equivalence relation obtained by ‘‘pushing $\sim_X$ forward under f’’. The remaining parts have you examine the relationship between the operations of pulling equivalence relations back, described in part (a), and of pushing them forward, just described.

(f) Show that if f is surjective, and one starts with an equivalence relation on Y, pulls it back via f to an equivalence relation on X as in part (a), and pushes that equivalence relation forward via f as in (e), then one gets the equivalence relation one started with.

(g) Show by example that if we remove the surjectivity assumption from (f), the conclusion can fail.

(h) Examine what conditions on f, if any, insure that if one starts with an equivalence relation on X, pushes it forward via f to an equivalence relation on Y, and pulls this back via f to an equivalence relation on X, the result is the original relation.

§0.3, ‘‘**Exercise 17**’’: Recall that the *Fibonacci numbers* are the sequence of integers f_n defined by the conditions $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all integers n. (This formula can be used to recursively evaluate f_n both for $n > 1$ and for $n < 0$, but for simplicity, we will only consider $n > 0$ in this exercise.)

(a) Show that if r and k are positive integers such that $r \mid f_k$, then for all $n \geq 0$,

$$f_{n+k} \equiv f_{k-1}\, f_n \pmod{r}.$$

(b) With the help of the above result, calculate the remainder on dividing f_{1000} by 17.

(An item near the end of this packet, ‘‘§13.1, Exercise 9’’, provides more detailed information on the behavior of the Fibonacci sequence modulo primes.)

§1.3, ‘‘**Exercise 21**’’: (a) Suppose a permutation $\sigma \in S_n$ is written as a product of disjoint cycles. Describe precisely how the expression of σ^2 as a product of disjoint cycles is related to that of σ.

(Your description should allow one to easily answer questions such as ‘‘If the expression for σ consists of i cycles of length 3, j cycles of length 6 and k cycles of length 12, how many cycles of each length will σ^2 have?’’ Of course, you must give a clear argument for why the result you assert is true.)

(b) Given a permutation $\sigma \in S_n$ written as a product of disjoint cycles, state a simple criterion for deciding whether σ is a square in S_n (i.e., whether there is a permutation ρ such that $\sigma = \rho^2$).

§1.3, ‘‘**Exercise 22**’’: This exercise was suggested by a student’s question in an earlier semester, asking whether there are any special conditions under which the product of two cycles in S_n is a cycle.

Let n be a positive integer, and let $\sigma = (a_1 \dots a_s)$, $\tau = (b_1 \dots b_t)$ be cycles in S_n, with $s, t > 1$. We know that if σ and τ are disjoint, then $\sigma\tau$ is not a cycle. (Namely, we have seen that it can be written in a unique way as a product of disjoint cycles, and its expression as the product of σ and τ is such a way, so it can’t *also* be a product of ‘‘just one cycle’’, i.e., a cycle itself.) We now consider the case where these cycles are one step away from being disjoint.

(a) Suppose $\{a_1, \dots, a_r\}$ and $\{b_1, \dots, b_s\}$ have one and only one element in common, $a_i = b_j$. Show that $\sigma\tau$ is then a cycle; in fact, write it in cycle form. (For simplicity in doing this, assume to begin with that a_i is not the first or the last term in the list $a_1, \dots, a_r$, and that b_j is not the first or the last term in the list $b_1, \dots, b_s$. The cases where one or both are first or last in their lists really work the same way, but some of the expressions like ‘‘$a_1, \dots, a_{i-1}$’’ that come up in your formula may then be empty.) What is the order of this cycle?

The next case, where $\{a_1, \dots, a_r\}$ and $\{b_1, \dots, b_s\}$ have two elements in common, is a bit more complicated. Let us call elements a_i and $a_{i'}$ ‘‘adjacent’’ in the cycle σ if one of them is carried to the other by σ; i.e., if either $|i - i'| = 1$ or $\{i, i'\} = \{1, r\}$, and define adjacency of b_j and $b_{j'}$ in τ analogously.

(b) Suppose $\{a_1, \dots, a_r\}$ and $\{b_1, \dots, b_s\}$ have exactly two elements in common, $a_i = b_j$ and $a_{i'} = b_{j'}$. Show that if a_i and $a_{i'}$ are not adjacent in σ and b_j and $b_{j'}$ are not adjacent in τ, then $\sigma\tau$ is a product of two disjoint cycles (hence not itself a cycle).

(c) Investigate the situation in which $(a_1 \dots a_s)$ and $(b_1 \dots b_t)$ again have two elements in common, but where these are adjacent in one or both cycles. The behavior may depend on which of a pair of adjacent elements precedes the other in σ and/or τ. You will find that some of these cases behave like (b) above, while others do not.

(d) Investigate the situation in which the cycles σ and τ have exactly three elements in common. (Here more complications come in: along with possibilities involving adjacency, there is the order in which the three elements appear in σ on the one hand and τ on the other.)

§1.3, ‘‘**Exercise 23**’’: Suppose Ω is a set, and $\sigma \in S_\Omega$ is a permutation which moves exactly n elements, for some nonnegative integer n. (I.e., such that $|\{ s \in S \mid \sigma(s) \neq s \}| = n$.) Let τ be any element of S_Ω. (Thus, τ may move finitely *or* infinitely many elements.) Show that $\sigma\tau\sigma^{-1}\tau^{-1}$ moves $\leq 2n$ elements.

§1.6, ‘‘**Exercise 27**’’: If G_1 and G_2 are groups, let us (for the purposes of this exercise) define a ‘‘weak isomorphism’’ from G_1 to G_2 to mean a bijection $\varphi\colon G_1 \to G_2$ such that for all $a, b, c \in G_1$ one has $\varphi(a b^{-1} c) = \varphi(a)\, \varphi(b)^{-1} \varphi(c)$.

(a) Show by example that a weak isomorphism between groups need not be an isomorphism.

(b) Show, however, that if there exists a weak isomorphism between G_1 and G_2, then there exists an isomorphism between them.

Note that our definition of a weak isomorphism φ says that φ ‘‘respects’’ the map taking three elements a, b, c to the element $a b^{-1} c$. Given any set H, a map $H \times H \times H \to H$ is called a *ternary* operation on H. We now ask

(c) Suppose H is a set and that we are given a ternary operation on H, which takes elements $a, b, c \in H$ to an element which we will denote $[a, b, c] \in H$. Can you find necessary and sufficient conditions on this operation for there to exist a group operation on H such that our ternary operation can be described by $[a, b, c] = a b^{-1} c$?

§2.2, ‘‘**Exercise 15**’’: (a) If a group G acts on a set S, and if T is a subset of S, show that the sets $\{g \in G \mid gT \subseteq T\}$ and $\{g \in G \mid gT \supseteq T\}$ are both closed under composition, and contain 1, and that their intersection, $\{g \in G \mid gT = T\}$, is a subgroup of G.

This leads us to wonder whether the two sets described above are themselves subgroups. We will answer this with the help of an example. For any two real numbers m and b with $m \neq 0$, let $a_{m,b}$ be the set-map $\mathbb{R} \to \mathbb{R}$ defined by $a_{m,b}(x) = mx + b$.

(b) Show that the set G of such maps forms a group under composition.

(c) Let us regard G as acting on $\mathbb{R}$ in the obvious way, by letting $a_{m,b} \cdot x = a_{m,b}(x)$. Determine the sets $\{g \in G \mid g\mathbb{Z} \subseteq \mathbb{Z}\}$ and $\{g \in G \mid g\mathbb{Z} \supseteq \mathbb{Z}\}$, and show that neither of them is a subgroup of G.

This example is also related to the normalizer construction:

(d) Let $t \in G$ denote the element $a_{1,1}$, and $H \leq G$ denote the subgroup $\langle t \rangle$. Show that the sets $\{g \in G \mid gHg^{-1} \subseteq H\}$ and $\{g \in G \mid gHg^{-1} \supseteq H\}$ also fail to be subgroups of G, but that their intersection is the subgroup $N_G(H)$. (Suggestion: Prove first that for any $a_{m,b} \in G$ and $r \in \mathbb{R}$, one has $a_{m,b}\, a_{1,r}\, (a_{m,b})^{-1} = a_{1,mr}$.)

§2.4, ‘‘**Exercise 21**’’: If m and n are nonzero integers, prove the equality of subgroups of $\mathbb{Z}$:

$$\langle m, n \rangle = \langle (m, n) \rangle.$$

§2.4, ‘‘**Exercise 22**’’: Let G be a group.

In parts (a)-(c) below, we will show that if A is a subset of G such that every two elements of A commute with each other, then the subgroup $\langle A \rangle$ of G is abelian.

This could be done using the description of the general element of $\langle A \rangle$ in terms of the generators (the elements of A): Given $g, h \in \langle A \rangle$, one could expand the product gh in terms of those generators, and show by a double induction that we can move the generators and inverses of generators in the expression for g, one by one, past each of the generators in the expression for h, ending up with the expression for hg, and obtaining equality. But the proof below will be simpler, and will give some further results (parts (d)-(f)).

(a) Show that if A and B are any two subsets of G, then the following three conditions are equivalent:

(i) For all $a \in A$, $b \in B$ we have $ab = ba$.

(ii) $A \subseteq C_G(B)$.

(iii) $\langle A \rangle \subseteq C_G(B)$.

(The proof should only take a few lines!)

(b) Deduce that the above equivalent conditions are also equivalent to

(iv) For all $a \in \langle A \rangle$ and $b \in \langle B \rangle$ one has $ab = ba$.

(Hint: Apply the result of (a) twice.)

(c) Deduce that if A is a subset of G such that for all $a, b \in A$ we have $ab = ba$, then $\langle A \rangle$ is abelian.

(d) Show that for any subgroup $H \leq G$, H is abelian if and only if $C_G(C_G(H))$ is abelian.

(e) In contrast, show by examples that the conditions ''H is abelian'' and ''$C_G(H)$ is abelian'' are independent; that is, that examples exist with all four possible combinations of truth-values for these two statements.

(f) Let H be a subgroup of G. We shall say H is a *maximal abelian subgroup* of G if H is abelian, but no subgroup of G properly containing H is abelian. Show that H is a maximal abelian subgroup of G if and only if $H = C_G(H)$.

§2.4, ''**Exercise 23**'': Within the group $S_{\mathbb{Z}}$ of all permutations of the integers, let F be the subgroup consisting of those permutations σ that move only finitely many elements (i.e., such that $\sigma(n) = n$ for all but finitely many integers n). Let $t \notin F$ be the permutation given by $t(n) = n+1$ for all n, and let

$$G = \langle F \cup \{t\} \rangle.$$

(a) Show that

$$G = \{\sigma \in S_{\mathbb{Z}} \mid (\exists\, k \in \mathbb{Z})\ \sigma(n) = n + k \text{ for all but finitely many } n \in \mathbb{Z}\}.$$

(b) Show that there exists a unique homomorphism $h: G \to \mathbb{Z}$ such that $h(t) = 1$. (Hint in proving uniqueness: elements of F have finite order.)

§2.4, ''**Exercise 24**'': Let X be a set, and $x \neq y$ two elements of X. Show that

$$\langle (S_X)_x \cup \{(x\ y)\} \rangle = S_X.$$

Here, following the notation of §2.2, $(S_X)_x$ denotes the stabilizer of x in S_X (regarding this group as acting, in the natural way, on X), and following the notation of §1.3, $(x\ y)$ is the cycle interchanging x and y, and fixing all other elements of X.

(We do not specify whether X is finite or infinite – the same argument will work in both cases.)

§2.5, ''**Exercise 4 (b)**'': How many generating pairs of elements does D_{16} have? (Once you have done Exercise 4, this is not much harder.)

§3.1, ''**Exercise 28 (b)**'': Like the present Exercise 28, but with ''*finite*'' deleted, and ''$gSg^{-1} \subseteq N$'' strengthened to ''$gSg^{-1} \cup g^{-1}Sg \subseteq N$''.

§3.1, ''**Exercise 29 (b)**'': Like the present Exercise 29, but with ''*finite*'' deleted, and ''$tSt^{-1} \subseteq N$'' strengthened to ''$tSt^{-1} \cup t^{-1}St \subseteq N$''.

§3.1, ''**Exercise 36, (b) and (c)**'': (b) Show by example that the condition ''$G/Z(G)$ is abelian'' does not imply that G is abelian.

(You might find it interesting to examine how the proof that $G/Z(G)$ cyclic implies G abelian fails to go over to this similar hypothesis.)

(c) Show that if $G/Z(G) \cong \mathbb{Q}$, then G is abelian.

§3.5, ‘‘**Exercise 2(b)**’’: Is it true conversely that for every n, the even permutations are precisely the squares in S_n? If this is not true in general, for which n is it true? Cf. ‘‘§1.3, Exercise 21’’.

§3.5, ‘‘**Exercise 10(b)**’’: Find a composition series for S_4. Deduce that S_4 is solvable.

§3.5, ‘‘**Exercise 18**’’: (a) If A is a set, describe a natural action of S_A on the set of *partitions* of A, indicating briefly why it satisfies the definition of an action.

(b) Show that if A has cardinality mn, where m and n are positive integers, and if we write $P_{m,n}$ for the set of partitions of A into n subsets of m elements each, then $P_{m,n}$ is carried into itself by the above action.

(c) Show that if $A = \{1,2,3,4\}$, then $|P_{2,2}| = 3$ and that every permutation of this 3-element set is induced (under the action described above) by a member of S_4. Thus, indexing the elements of $P_{2,2}$ by $\{1,2,3\}$, this action induces a surjective homomorphism $S_4 \to S_3$. Determine the kernel of this homomorphism; verify in particular that it is contained in A_4. This explains the result of §3.5, Exercise 9.

(d) Determine the stabilizer of a single element $a \in P_{2,2}$ under the above action of S_4. Letting $a = \{\{1,3\}, \{2,4\}\}$, show that this group can be identified with the group D_8 of symmetries of a square with vertices labeled 1, 2, 3, 4. Can you explain geometrically why this is so?

§3.5, ‘‘**Exercise 19**’’: Find an infinite set Ω, and permutations $\alpha, \beta \in S_\Omega$ such that $\alpha\beta\alpha^{-1}\beta^{-1}$ is a transposition.

§4.1, ‘‘**Exercise 8(c)**’’: Show that for all odd primes p, the group D_{2p}, regarded as a group of permutations of the vertices of a regular p-gon, is primitive, but that it is doubly transitive only when $p = 3$. (Thus, the case $p = 3$ is an example of part (a), while all other such cases are examples showing that the converse of that statement is false.)

§4.1, ‘‘**Exercise 11**’’: Let G be a group. A set A given with an action of G on it is often called a *G-set*, and we shall use that language here. If A and B are G-sets, a *homomorphism* from A to B (as G-sets) will mean a map $\varphi: A \to B$ such that for all $g \in G$ and $a \in A$, one has $\varphi(ga) = g\,\varphi(a)$.

(Note that while the concept of a homomorphism of groups involves two groups, this concept involves a single group G, and two G-sets. If you have had linear algebra, this is like the concept of linear map of vector spaces, where one considers two vector spaces over the *same* field.)

We shall call G-sets A and B isomorphic if there exists an isomorphism, i.e., an invertible homomorphism, between them.

Given a G-set A and an element $a \in A$, the orbit $\{ga \mid g \in G\}$ may be considered a G-set (‘‘the sub-G-set of A generated by a’’. Most texts write this orbit, logically, as Ga. Our authors avoid that notation, probably because of the danger of confusion with the symbol G_a for the stabilizer subgroup.)

Show that for any G-set A, each orbit in A is isomorphic, as a G-set, to the G-set of left cosets of some subgroup $H \le G$. (Hint: Taking any $a \in A$, use Theorem 3, p.119, to determine what H must be if the desired homomorphism is to take $1H$ to a; and then show that this choice of H works.)

§4.1, ‘‘**Exercise 12**’’: Again let G be a group, and let us use the definitions of the first paragraph of the preceding exercise. Let us call a G-set A ‘‘transitive’’ if the action of G on A is transitive in the sense given in our text.

Let A and B be transitive G-sets, and $a \in A$, $b \in B$ any elements.

(a) Show that if there exists a homomorphism $A \to B$ taking a to b, then there is only one such homomorphism, and it is surjective.

(b) Obtain a necessary and sufficient condition for a homomorphism as in (a) to exist, in terms of the relation between the stabilizer subgroups G_a and G_b.

§4.1, ‘‘**Exercise 13**’’: Let G be a group, and let us continue to use the language introduced in the first paragraphs of the two preceding exercises.

(a) If A and B are G-sets, show that the set $A \times B = \{(a,b) \mid a \in A,\ b \in B\}$ becomes a G-set if we define $g(a,b) = (ga, gb)$ for all $g \in G$, $(a,b) \in A \times B$.

(b) Show that if A and B are both finite transitive G-sets, and if g.c.d.$(|A|, |B|) = 1$, then the G-set $A \times B$ is also transitive. (Suggestion: For $a \in A$, $b \in B$, consider the relations among the indices $|G : G_a|$, $|G : G_b|$, and $|G : G_{(a,b)}|$.)

(c) On the other hand, show that if A is a G-set with more than one element, then the G-set $A \times A$ is never transitive.

(d) Show that if A and B are G-sets and a an element of A, then the G-set $A \times B$ is transitive if and only if A is transitive, and the action of the subgroup G_a on B is transitive.

(e) Deduce from (b) and (d) that if B is a finite transitive G-set, and H is a subgroup of finite index in G such that $|G : H|$ is relatively prime to $|B|$, then B is also transitive as an H-set. (Suggestion: Let A be the G-set of left cosets of H.)

§4.1, ‘‘**Exercise 14**’’: Let A be a transitive G-set and a an element of A. An *automorphism* of A (as a G-set) means an isomorphism of A with itself. It is easy to see that the composite of two automorphisms is an automorphism, and that the set of automorphisms of A forms a group, $\mathrm{Aut}(A)$, under composition. (This notation is analogous to that of the Definition on p.133, but that definition refers to automorphisms of groups, while here we are talking about automorphisms of G-sets. One can similarly define the group $\mathrm{Aut}(X)$ for any sort of mathematical object X.)

(a) Determine the structure of $\mathrm{Aut}(A)$ in terms of the subgroup $G_a \leq G$. (First step: use the idea of §4.1, ‘‘Exercise 11’’, together with §4.1, Exercise 1, to determine which elements $ga \in A$ an automorphism of A can carry a to.)

For the next part, we note that a homomorphism from a mathematical object to that same object is called an *endomorphism* of the object. (So the automorphisms are the invertible endomorphisms.) The set of endomorphisms of a mathematical object X is written $\mathrm{End}(X)$; this set is closed under composition, and contains the identity, but its elements may not have inverses. A system of elements with an associative multiplication and an identity element (but whose elements need not all be invertible) is called a *monoid*.

(b) Determine the structure of $\mathrm{End}(A)$, again in terms of the subgroup $G_a \leq G$. (Because we have not studied monoids, you won’t have ready-made symbolism in terms of which to describe $\mathrm{End}(A)$ as you did for $\mathrm{Aut}(A)$; but you can describe its members in terms of certain equivalence classes of certain elements of G, and then describe how they are composed. Before attempting this, you should stop and think: if an endomorphism of a transitive G-set is not an automorphism, can this be because it is not one-to-one, or because it is not onto, or can both happen?)

(c) As in ‘‘§2.2, Exercise 15’’, let us, for any two real numbers m and b, with $m \neq 0$ define $a_{m,b}$ be the set-map $\mathbb{R} \to \mathbb{R}$ given by $a_{m,b}(x) = mx+b$; and let G be the group of all such maps, under composition. Let $H \leq G$ be the subgroup of G consisting of the maps $a_{1,n}$ with $n \in \mathbb{Z}$, and let A be the G-set of left cosets of H in G. Show that $\mathrm{End}(A)$ is strictly larger than $\mathrm{Aut}(A)$.

§4.3, ‘‘**Exercise 5′**’’: Suppose $1 < |G:Z(G)| = n < \infty$, and let p be the least prime dividing n. Show that every conjugacy class of elements of G has at most n/p elements. (Suggestion: first take care of the 1-element conjugacy classes.)

§4.3, ‘‘**Exercise 27′**’’: Let G be a finite group, and let $g_1, g_2, \ldots, g_r \in G$ be representatives of its nonidentity conjugacy classes.

(a) Show that $\langle g_1, g_2, \ldots, g_r \rangle = G$. (Hint: apply Exercise 24 to $\langle g_1, g_2, \ldots, g_r \rangle$.)

(b) Deduce the result of Exercise 27 as stated in the text.

§4.3, ‘‘**Exercise 37**’’: Let G be a group.

Show that for any two elements $g, h \in G$, the products gh and hg are conjugate in G. Conversely, show that if $x, y \in G$ are conjugate elements, then there exist $g, h \in G$ such that $x = gh$ and $y = hg$.

§4.5, ‘‘**Exercise 57**’’: (a) Show that if G is a nonabelian group of order 21, then it can be described as

$$\langle r, s \mid r^7 = 1,\ s^3 = 1,\ sr = r^2 s \rangle .$$

(Hint: The above equation relating r and s can be written $srs^{-1} = r^2$. For arbitrary r of order 7 and s of order 3 in G, show that srs^{-1} must either equal r^2, or a certain other power of r. In the latter case, replace s by the other nonidentity element of $\langle s \rangle$.)

(b) Show that there is indeed a nonabelian group of order 21. (Suggestion: Look for elements satisfying the above relations within S_7.)

§4.5, ‘‘**Exercise 58**’’: Let G be a group, and p and q distinct primes.

(a) If a Sylow p-subgroup of G normalizes a Sylow q-subgroup of G, must it normalize every Sylow q-subgroup of G?

(b) If a Sylow p-subgroup of G centralizes a Sylow q-subgroup of G, must it centralize every Sylow q-subgroup of G?

§5.1, ‘‘**Exercise 19**’’: (a) For p and n as in Exercise 11, find a formula for the number of subgroups of order p^2 in E_{p^n}.

(b) The formula in (a) can be written as a fraction with a polynomial in p as numerator, and with $p+1$ as denominator. Can you show that $p+1$ must divide the numerator, without appealing to the fact that the expression represents the answer to a counting problem?

§5.1, ‘‘**Exercise 20**’’: Suppose A is a group having a presentation in terms of m generators and m' relations,

$$A = \langle x_1, \ldots, x_m \mid u_i(x_1, \ldots, x_m) = 1 \ \ (i = 1, \ldots, m') \rangle,$$

and B a group with a presentation in terms of n generators and n' relations,

$$B = \langle y_1, \ldots, y_n \mid v_j(y_1, \ldots, y_{n'}) = 1 \ \ (j = 1, \ldots, n') \rangle.$$

Show that $A \times B$ can be presented using $m+n$ generators and $m'+n'+mn$ relations, namely

$$A \times B \;=\; \langle\, x_1, \ldots, x_m, y_1, \ldots, y_n \;\mid\; u_i(x_1, \ldots, x_m) = 1,\;\; v_j(y_1, \ldots, y_n) = 1,\;\; x_r\, y_s\, x_r^{-1} y_s^{-1} = 1 \,\rangle,$$

where on the right-hand side, i, j, r, s range from 1 to m', n', m, n respectively.

§5.2, ‘‘**Exercise 17**’’: Let p be a prime.

(a) Show that $Z_{p^2} \times Z_p$ has exactly $2p+4$ subgroups. Draw the lattice diagram of this group for $p = 2,\ 3.$

(b) Show that $Z_{p^2} \times Z_p$ has exactly 4 characteristic subgroups, regardless of p. Mark these in the lattice diagrams of part (a).

(c) Try to determine the number of subgroups and the number of characteristic subgroups of $Z_{p^n} \times Z_{p^m}$ for general $0 < m < n$.

(d) Do the answers to part (c) change if we allow $m = n$ and/or $m = 0$?

§5.4, ‘‘**Exercise 21**’’: Let P be a p-group.

(a) Show that every nontrivial normal subgroup N of P has nontrivial intersection with $Z(P)$.

This shows, in particular, that if P is noncommutative, so that $P' \neq 1$, then $P' \cap Z(P) \neq 1$. Recall, however, that though P' is generated by commutators $[g, h]$, it does not consist of such commutators. Hence part (a) does not directly yield:

(b) Show that if P is noncommutative, then there exists a commutator $[g, h] \neq 1$ lying in $Z(P)$.

However, there is an easy proof of (b) from other results we have had.

§5.4, ‘‘**Exercise 22**’’: (a) Show that for any group G and subset A, one has $[A, G] \trianglelefteq G$.

(b) Show, more generally, that if G is a group, H a subgroup, and A a subset of G, then $H \leq N_G([A, H])$. If you do this part, then instead of doing part (a) from scratch, you may simply show how that result is a special case of this one.

(c) In the situation of part (b), is it also true that $A \subseteq N_G([A, H])$?

(d) In the situations of parts (a) and (b), is it in general true that $[A, G] = [\langle A\rangle, G]$? That $[A, H] = [\langle A\rangle, H]$?

§5.4, ‘‘**Exercise 23**’’: (a) Show that for any group G and subsets A and B, one has $[A, B] = [B^{-1}, A^{-1}]$. (Here A^{-1} means $\{a^{-1} \mid a \in A\}$, and B^{-1} is defined analogously.)

(b) Show by examples that in the situation of part (a), of the 8 commutator expressions that one can obtain from $[A, B]$ by reversing the positions of the two terms in the bracket, and/or attaching ‘‘$^{-1}$’’ to the first of those terms, and/or attaching it to the second, none of the 6 other than $[A, B]$ and $[B^{-1}, A^{-1}]$ need represent the same subgroup of G as those two.

(c) Show that the group of operations on commutator *expressions* generated by the three operations described in part (b) (where the operation of ‘‘attaching $^{-1}$ to an expression’’ is understood, if that symbol already wears a ‘‘$^{-1}$’’, to mean removing that symbol), is isomorphic to D_8, and that if one considers two commutator expressions equivalent if they always represent the same subgroup, then the induced action of that group on the equivalence classes has for kernel the center of D_8.

(d) Investigate how the result of part (b) changes if A and/or B is assumed a subgroup of G.

§5.5, ‘‘**Exercise 26**’’: Let G be any group. For each $g \in G$ let $\lambda_g \in S_G$ denote the left-translation map $h \mapsto gh$, and $\rho_g \in S_G$ the right-translation map $h \mapsto hg$. (Here S_G denotes the group of all permutations of the elements of G.) Let H be the subgroup of S_G generated by $\mathrm{Aut}(G) \cup \{\lambda_g \mid g \in G\}$; i.e., by all automorphisms of the group G, and all left translation maps.

(a) Show that $H \cong \mathrm{Hol}(G)$.

(b) Show that the subgroup of S_G generated by all left translation maps λ_g and all right translation maps ρ_g $(g \in G)$ is a subgroup of H. Describe this subgroup as a semidirect product, in a way analogous to the definition of $\mathrm{Hol}(G)$.

§5.5, ‘‘**Exercise 27**’’: (a) Show by example that the result of Exercise 6 (p.184) becomes false if the assumption that K is cyclic is removed. (Hint: You can get an example where K is finite abelian.)

(b) Show by example that the result of that exercise, with K cyclic as in the original statement, becomes false if the assumption that if K is infinite, then φ_1 and φ_2 are injective is removed. (Hint: You can get an example where H is cyclic of prime order.)

(c) Show, however, that the result again becomes true if, after removing both the above assumptions, one strengthens the assumption that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate in $\mathrm{Aut}(H)$ to say that $\varphi_1 = \alpha\varphi_2$ for some inner automorphism α of $\mathrm{Aut}(H)$.

§5.5, ‘‘**Exercise 28**’’: Suppose that K is an *abelian* group, H is any group, and $\varphi\colon K \to \mathrm{Aut}(H)$ a homomorphism.

(a) Show that a homomorphism $\theta\colon K \to \mathrm{Aut}(H \rtimes_\varphi K)$ can be defined by

$$\theta(k')((h,k)) \;=\; (\varphi(k')(h),\, k).$$

(b) Show that

$$(H \rtimes_\varphi K) \rtimes_\theta K \;\cong\; (H \rtimes_\varphi K) \times K.$$

(Once you find what the isomorphism should be, the rest will be easy.)

This shows that a given group G can be put together in different ways from the same pieces. E.g., since S_3 can be written $Z_3 \rtimes Z_2$ using an appropriate action of Z_2 on Z_3, the above isomorphism shows that a semidirect product $S_3 \rtimes Z_2$ formed using a nontrivial action of Z_2 on S_3 is isomorphic to $S_3 \times Z_2$, the semidirect product formed using the trivial action.

§5.5, ‘‘**Exercise 29**’’: Show that the group $G = S_3 \times S_3$ has two cyclic subgroups $\langle x \rangle$ and $\langle y \rangle$, each of order 6, such that $G = \langle x \rangle \langle y \rangle$, but that G is not a semidirect product of any two such subgroups.

§5.5, ‘‘**Exercise 30**’’: Let G be a group and H a subgroup. Show that H is a *characteristic* subgroup of G if and only if for every group K containing G as a normal subgroup, H is also a normal subgroup of K.

(In constructing examples of groups K containing G, you may simply obtain a one-to-one homomorphism $\varphi\colon G \to K$, and regard G as identified with its image $\varphi(G)$, each element $g \in G$ being identified with $\varphi(g)$. This can be justified formally – i.e., one can show that whenever one has such a homomorphism, one can construct an isomorphic copy of K which literally contains G in the indicated way – but we won’t go into details about this.)

§6.3, ‘‘**Exercise 14**’’: Let F be the free group on a set of distinct generators x_i $(i\in\mathbb{Z})$.

(a) Show that F has a unique automorphism α satisfying $\alpha(x_i) = x_{i+1}$ for all $i\in\mathbb{Z}$.

Now let $\langle y\rangle$ be an infinite cyclic group, and $\varphi\colon \langle y\rangle \to \mathrm{Aut}(F)$ the homomorphism taking y to α.

(b) Show that $F \rtimes_{\varphi} \langle y\rangle$ is a free group on the two generators x_0 and y. (If you consider ‘‘the’’ free group on a set of generators to be given by the construction in our text, then what you are to prove is that the homomorphism from the free group on two generators s and t to the semidirect product described above that takes s to x and t to y is an isomorphism.)

§7.1, ‘‘**Exercise 31**’’: Let D be a nonsquare integer.

(a) Suppose m and n are integers such that $m+n\sqrt{D}$ is a unit of $\mathbb{Z}[\sqrt{D}]$. Show that $m-n\sqrt{D}$ is also a unit of that ring, and that $m^2-n^2 D = \pm 1$ in $\mathbb{Z}$. Conversely, show that if m and n are integers such that $m^2-n^2 D = \pm 1$ in $\mathbb{Z}$, then $m+n\sqrt{D}$ and $m-n\sqrt{D}$ are units of $\mathbb{Z}[\sqrt{D}]$.

(b) Suppose that $D > 0$ and that $m+n\sqrt{D}$ is a unit of $\mathbb{Z}[\sqrt{D}]$ with $n \neq 0$. Show that $m+n\sqrt{D}$ and $m-n\sqrt{D}$ have different absolute values in $\mathbb{R}$, and deduce that the unit $m+n\sqrt{D}$ of $\mathbb{Z}[\sqrt{D}]$ has infinite order in the group $\mathbb{Z}[\sqrt{D}]^{\times}$.

(c) Deduce that for D a positive nonsquare integer, if the equation $m^2-n^2 D = 1$ has an integer solution with $n \neq 0$, then it has infinitely many such solutions.

(d) Using the idea of part (c), find 10 solutions to $n^2 - 2m^2 = 1$ in positive integers m and n.

(e) On the other hand, if $D < 0$, show that $\mathbb{Z}[\sqrt{D}]^{\times}$ is a finite group.

(f) Prove results analogous to (b), (c) and (e) for rings $\mathbb{Z}[(1+\sqrt{D})/2]$ where $D \equiv 1 \pmod 4$. (To do this, you need to figure out the right analog of $m^2-n^2 D$ for an element $m + n(1+\sqrt{D})/2$.)

(g) Using the idea of (f), find 10 solutions to the equation $n^2 - mn - m^2 = 1$ in positive integers m and n. What do you notice about these solutions?

§7.2, ‘‘**Exercise 14**’’: Let A be the additive group of $\mathbb{R}[x]$ (the ring of polynomials over the real numbers), and let E denote the endomorphism ring of A (the ring constructed in §7.1, Exercise 29). Within E, let X be the element which acts by multiplication by $x\in\mathbb{R}[x]$; i.e., $X(p(x)) = x\,p(x)$, and let D be the element which acts by differentiation; i.e., $D(p(x)) = dp(x)/dx$. (That X is indeed an endomorphism of the abelian group A is clear from the distributive law in $\mathbb{R}[x]$; that D is such an endomorphism can be seen from the sum rule for differentiation.)

Prove that in E we have $DX = XD + 1_E$. You may use standard facts from calculus. I am writing 1_E for the identity element of E, so that in your computations, there will be no confusion between it and the polynomial $1\in\mathbb{R}[x]$. (Ordinarily, this result would be written $DX = XD + 1$, or $DX = XD + I$ where I is a common symbol for the identity operator on a vector space.)

§7.3, ‘‘**Exercise 38**’’: (Cayley’s Theorem for rings with 1.) Let R be a ring with identity, and let E be the endomorphism ring of the additive group of R (the ring constructed in §7.1, Exercise 29). For each $r\in R$, let $\varphi(r)\colon R \to R$ be the map given by $\varphi(r)(s) = rs$ $(s\in R)$.

Show that for every $r\in R$, $\varphi(r)$ is a member of E. (In ‘‘§7.2, Exercise 14’’ above, the reason for a particular case of this fact was mentioned; here you are asked to show the straightforward calculation.)

Show that φ gives a one-to-one ring homomorphism $R \to E$.

Thus, every ring with 1 is isomorphic to a subring of the ring of endomorphisms of some abelian group.

§7.3, ‘‘**Exercise 39**’’: Suppose R is a ring not necessarily having 1. We would like to know whether we can embed it in a ring with 1. If we had some ring with 1 containing R, then on combining the element 1 with the elements of R under repeated application of the ring operations, it is not hard to see that all elements we could get would reduce to the form $n\cdot 1 + r$ $(n\in\mathbb{Z},\ r\in R)$. We can’t say whether some pairs of distinct expressions of this form might be equal, but making the simplest assumption, that they are not, we can figure out how to perform the ring operations on such expressions, and then try to model the resulting structure. Let us show that this does, indeed give a ring with 1 containing R.

Define R^1 to be the set $\mathbb{Z}\times R$ (where $(n,r)\in\mathbb{Z}\times R$ is intended to model $n\cdot 1+r$). Let us give it the additive structure of the direct product of the additive groups of $\mathbb{Z}$ and R,

$$(m,r) + (n,s) \;=\; (m+n,\ r+s).$$

The preceding considerations suggest that we should give R^1 the multiplication described by

$$(m,r)\,(n,s) \;=\; (mn,\ ms+nr+rs).$$

Here, ms and nr are defined as on p.20, sentence before Proposition 2, using the additive group structure of R.

(a) Show that these operations indeed make R^1 a ring with 1.

(b) Show that the elements $(0,r)$ form a subring of R^1 that is isomorphic to R.

So every ring is indeed isomorphic to a subring of a ring with identity. (Combining with the preceding exercise, we see that every ring can be embedded in the endomorphism ring of an abelian group.)

But there is a down side to the above construction:

(c) If R already had an identity 1, show that the image of this element in R^1 under the isomorphism of (b) is not an identity element for R^1.

§7.4, ‘‘**Exercise 42**’’: If in §7.4, Exercise 8, one merely assumes R a commutative ring with 1 (not necessarily an integral domain), show that one direction of the stated ‘‘if and only if’’ conclusion remains true, but show by example that the other direction fails.

§7.4, ‘‘**Exercise 43**’’: Let R be a commutative ring with 1, and a an element of R. Show that the following conditions are equivalent.

(i) a is a unit of R.

(ii) a is not contained in any proper ideal of R.

(iii) a is not contained in any prime ideal of R.

(iv) a is not contained in any maximal ideal of R.

§7.4, ‘‘**Exercise 44**’’: Let R be a commutative ring with 1, and D a nonempty subset of R that is closed under multiplication, and does not contain the element 0. Let A be the partially ordered set of all ideals of R that contain no members of D, and let us consider A to be partially ordered by inclusion.

(a) Show that A has a maximal element.

(b) Show that any such maximal element is a prime ideal of R.

(c) Show by example that a maximal element of A need not be a maximal ideal of R.

The result of (a) and (b) gives ways of obtaining prime ideals with specified properties. For instance,

(d) Given $x \in R$, show that if no power of x is equal to 0, then there is a homomorphism of R into an integral domain that does not have x in its kernel. Is the converse true?

§7.4, ‘‘**Exercise 45**’’: Let I be a set, and for each $i \in I$, let R_i be a commutative nonzero ring with unity. Let R be the ring $\Pi_{i\in I} R_i$, with componentwise operations. The general element of R may be written $r = (r_i)_{i\in I}$, where for each i, $r_i \in R_i$ denotes the i-th component of r. One may abbreviate $(r_i)_{i\in I}$ to (r_i) when there is no danger of ambiguity.

We note that for any $j \in I$ and any ideal A of R_j, the set of elements of R whose j-th component lies in A will be an ideal of R. Let us call this the ideal of R ‘‘induced by’’ the ideal A of R_j.

(a) If A' is the ideal of R induced by an ideal $A \subseteq R_j$, show that $R/A' \cong R_j/A$. Deduce that if A is prime in R_j, then A' is prime in R.

(b) Show that if B is a prime ideal of R, and I is finite, then B is induced by a prime ideal of one of the rings R_i; but show by example that this is *not* in general true of non-prime ideals.

(c) On the other hand, show that if I is infinite, then there always exist prime ideals of R which are not induced by any ideal of any of the R_i.

§7.4, ‘‘**Exercise 46**’’: This exercise explores further the ideas begun in the previous exercise. Let the rings R_i and R be as in that exercise. For any subset $J \subseteq I$, let $R_J = \Pi_{i\in J} R_i$. Thus, we have a natural homomorphism $R \to R_J$ taking each element $(r_i)_{i\in I}$ to $(r_i)_{i\in J}$, i.e., dropping those components r_i such that $i \notin J$.

Let us say an ideal A of R *lives on* J if it is the inverse image, under the above map, of an ideal of R_J. Thus, the last part of the preceding exercise shows that if I is infinite, then R has prime ideals which do not live on any one-element subset of I.

(a) Show that if J_1, J_2 are subsets of I such that $I = J_1 \cup J_2$, then every *prime* ideal of R either lives on J_1 or lives on J_2. Show, however, that this is not in general true of non-prime ideals.

(b) Let P be a prime ideal of R, and let $U_P = \{J \subseteq I \mid P$ lives on $J\}$. What properties can you prove that the set U_P must have? Can you find necessary and sufficient conditions on a set U of subsets of I for there to exist a prime ideal $P \subseteq R$ such that $U = U_P$?

§7.5, ‘‘**Exercise 7**’’: Here is an alternative development of the ring $Q = D^{-1}R$ of Theorem 7.5, which takes more work to start up, but where, once this is done, the computations are more natural.

We begin with a definition. If R is a commutative ring and I an ideal of R, we shall call a function $\varphi: I \to R$ *R-linear* if it is a homomorphism of additive groups, and if for every $r \in R$ and $x \in I$ we have $\varphi(rx) = r\varphi(x)$. (More generally, this definition is used for commutative or noncommutative R and any map $\varphi: A \to B$ where A and B are abelian groups on which R acts by endomorphisms. Abelian groups with such structure are called ‘‘R-modules’’, and R-linear maps among them are called homomorphisms of R-modules. Modules are studied in Chapters 10-12.)

Now let R and D be as in Theorem 7.15. Let us define a *D-map* to mean an R-linear map φ: $(d) \to R$ for some $d \in D$. (This is an ad hoc name made up for this exercise.) Let us call D-maps φ_1: $(d_1) \to R$ and $\varphi_2: (d_2) \to R$ *equivalent* if there exists a common multiple $d_3 \in D$ of d_1 and d_2 such that the restrictions of φ_1 and φ_2 to (d_3) are equal.

(For intuition, consider the case where $R = \mathbb{Z}$ and $D = \mathbb{Z} - \{0\}$. Then we can think of $2/10$ as the function $10\mathbb{Z} \to \mathbb{Z}$ taking $10n$ to $2n$ for all n, and $3/15$ as the function $15\mathbb{Z} \to \mathbb{Z}$ taking $15m$ to $3m$ for all m. We consider these equivalent because they agree on multiples of 30.)

(a) Show that if, as above, for some common multiple d_3 of d_1 and d_2 in D the restrictions of φ_1 and φ_2 to (d_3) are equal, then for *every* common multiple d of d_1 and d_2, the restrictions of φ_1 and φ_2 to (d) are equal.

(b) Show that the relation of equivalence of D-maps described above is an equivalence relation.

We now let Q denote the set of equivalence classes of D-maps under this relation.

We would like to define addition on Q as follows. Given $q_1, q_2 \in Q$, choose any $d \in D$ such that the equivalence class of q_1 has a member $\varphi_1\colon (d) \to R$ and the equivalence class of q_2 has a member $\varphi_2\colon (d) \to R$. Then define $\varphi_3\colon (d) \to R$ by $\varphi_3(x) = \varphi_1(x) + \varphi_2(x)$ for all $x \in (d)$, and let $q_1 + q_2$ be the equivalence class of φ_3.

(c) Show that given q_1 and q_2, there indeed exists d such that both equivalence classes have members with domain (d), and that the above definition of gives a *well-defined* binary operation ‘‘+’’ on Q.

We now come to a step that was hard in the book’s development, but is easy in ours:

(d) Show that Q is a group under the above operation of addition.

Multiplication, next: Given $q_1, q_2 \in Q$, we choose $d_1, d_2 \in D$ such that the equivalence class q_2 has a member φ_2 which is defined on (d_2), with $\varphi_2(d_2) \subseteq (d_1)$, and q_1 has a member φ_1 which is defined on (d_1). We then define $q_1 q_2$ to be the equivalence class of the composite map $\varphi_1 \varphi_2$.

(e) Show that the choices described above can always be made, and the result is a well-defined operation.

(f) Show that under the two operations described above, Q is a commutative ring. (Again, each step will be easier than for the book’s construction.)

(g) Describe a one-to-one ring homomorphism $R \to Q$.

(h) Show that the ring Q and this homomorphism have the properties stated in Theorem 7.15. Deduce from that theorem that our Q is isomorphic to the Q of the theorem.

§7.6, ‘‘**Exercise 12**’’: Prove the following generalization of the two-ideal case of the Chinese Remainder to ideals that may not be comaximal. In stating it, we drop the assumption that R is commutative (which actually wasn’t needed in the book’s version, except to conclude that $A \cap B = AB$, which we don’t assert here).

(a) Let R be a ring with 1, let A and B be ideals of R, and let $x + A$, $y + B$ be elements of R/A and R/B respectively. Show that the following conditions are equivalent:

(i) There exists an element $z \in R$ such that $z + A = x + A$ and $z + B = x + B$.

(ii) $x - y \in A + B$.

(b) For $R = \mathbb{Z}$, translate the above result into a statement about solutions to simultaneous congruences.

§7.6, ‘‘**Exercise 13**’’: It would be nice to generalize the result of the preceding exercise to more than two ideals. For instance, suppose we are given ideals A_1, A_2 and A_3 of R, and elements $x_1 + A_1 \in R/A_1$, $x_2 + A_2 \in R/A_2$, $x_3 + A_3 \in R/A_3$. Will the following conditions be equivalent?

(i) There exists $z \in R$ such that $z + A_i = x_i + A_i$ for $i = 1, 2, 3$.

(ii) $x_i - x_j \in A_i + A_j$ for all $i, j \in \{1, 2, 3\}$.

Either prove the above statements equivalent, or find a counterexample.

§8.1, ‘‘**Exercise 13**’’: Let R be an integral domain.

If a and b are nonzero elements of R and d a common divisor of a and b, then it is easy to see that ab/d is a common multiple of a and b; and if d_1 and d_2 are two common divisors of a and b, we see that $d_1 \mid d_2$ if and only if $(ab/d_2) \mid (ab/d_1)$. Thus, it would appear that d should be a *greatest* common divisor of a and b (a common divisor that is a multiple of all other common divisors) if and only if ab/d is a *least* common multiple of a and b (a common multiple that is a divisor of all other common multiples).

But the above observations do not turn into a valid argument, because, although it is true that for every common divisor d of a and b the quotient ab/d makes sense, it is not true that for every nonzero common multiple e of a and b we can form the quotient ab/e in R. (We can do so in the field of fractions of R; but the result may or may not lie in R.) Rather, we have:

(a) Show that for nonzero $a, b \in R$, the map $d \mapsto ab/d$ gives a bijection

$$\{\text{common divisors } d \text{ of } a \text{ and } b\} \to \{\text{common multiples } e \text{ of } a \text{ and } b \text{ which divide } ab\},$$

having the property that a divisibility relation holds between two elements of the first set if and only if the reverse divisibility relation holds between their images in the second set.

(b) Deduce that if a and b have a least common multiple, then they have a greatest common divisor.

To see that the converse is not true, let F be any field, and within the polynomial ring $F[x]$, let $R = F[x^2, x^3]$ be the subring generated by F, x^2, and x^3; that is, the subring of all polynomials $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ such that $a_1 = 0$.

(c) Show that the above set R of polynomials is indeed the subring of $F[x]$ generated by F, x^2, and x^3. In this ring, let us call an element ax^n with a a nonzero member of F and n a nonnegative integer ($\neq 1$) a *monomial*. Show that the only divisors in R of a monomial ax^n are the monomials bx^m with either $m = n$ or $m \leq n-2$.

(d) Deduce that the monomials x^2 and x^3 have a greatest common divisor, but have no least common multiple.

(e) For which pairs of integers $m < n$ do x^m and x^n have a greatest common divisor in R? For which pairs do they have a least common multiple? Show that the statement that they have a greatest common divisor if and only if they have a least common multiple is valid for all but three such pairs.

(f) Show that for any nonzero elements a, b, c of an integral domain R, there is a least common multiple e of a and b if and only if there is a least common multiple of ac and bc, and that this will then be ec.

(g) Show that if an integral domain R has nonzero elements a and b with no least common multiple, then for some nonzero $c \in R$, the elements ac and bc will have no greatest common divisor. (Hint: use (a).)

It follows that, despite the result of (d) above, a ring has a pair of elements with no least common multiple if and only if it has a pair with no greatest common divisor.

§8.1, ‘‘**Exercise 14**’’: For a ring of fractions $D^{-1}R$ as in Theorem 15, show that if R is a Euclidean domain with a norm function N, then $D^{-1}R$ is a Euclidean domain with norm N', where for every nonzero $a \in D^{-1}R$ we define $N'(a)$ to be the minimum, over all $b \in aD^{-1}R \cap R$, of $N(b)$.

§8.3, ‘‘**Exercise 6(d)**’’: Show that in case (a) of §8.3, Exercise 6, the field described is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, that in case (c), both fields are isomorphic to $\mathbb{Z}/p\mathbb{Z}$, while in case (b), the field described contains a subfield F isomorphic to $\mathbb{Z}/q\mathbb{Z}$ and an element i whose square is -1, such that every element of the field can be written as $\alpha+\beta i$ for unique $\alpha, \beta \in F$.

§8.3, ‘‘**Exercise 12**’’: (a) Suppose D is a unique factorization domain which, up to associates, has only one irreducible element; i.e., which has an irreducible element p such that all irreducible elements of D are associates of p. Let v be the function which takes each nonzero element $a \in D$ to the unique nonnegative integer α such that a can be written $u\,p^{\alpha}$ for some unit u of D. Show that the function v can be extended to the field of fractions of D so as to be a discrete valuation in the sense of §7.2, Exercise 26 (p.232), and that the valuation ring of v will then be D. Thus, by Example (4) on p.272, D is a Euclidean domain, and hence a principal ideal domain.

The above is fairly easy. The generalization below requires ingenuity; but once one has found the right tricks, the proof is not too hard.

(b) Suppose D is a unique factorization domain which, up to associates, has only finitely many irreducible elements; i.e., which has irreducible elements $p_1, \ldots, p_n$ such that every irreducible element of D is an associate of one of $p_1, \ldots, p_n$. Again show that D is a Euclidean domain, and hence a principal ideal domain.

(In doing (b) it will again be useful to define the functions $v_1, \ldots, v_n : D-\{0\} \to \mathbb{N}$ such that every $a \in D-\{0\}$ can be written $u\,p_1^{v_1(a)} \ldots p_n^{v_n(a)}$. These v_i are called the *valuations* on D associated with the irreducible elements p_i.)

§8.3, ‘‘**Exercise 13**’’: A 3-tuple (a, b, c) of positive integers is called a *Pythagorean triple* if $a^2 + b^2 = c^2$, i.e., if it represents the three sides of a ring triangle, as described by the Pythagorean Theorem. A Pythagorean triple (a, b, c) is called *primitive* if a, b and c have no common divisor. (So starting with the primitive Pythagorean triples, one gets all Pythagorean triples by multiplying by all positive integers.)

(a) Show that an integer c is the third term of a primitive Pythagorean triple if and only if $c > 1$ and all primes dividing c are $\equiv 1 \pmod 4$.

(b) If $c = p_1^{n_1} \ldots p_k^{n_k}$ where $p_1, \ldots, p_k$ are primes each congruent to $1 \pmod 4$, and $n_1, \ldots, n_k$ are positive integers, how many primitive Pythagorean triples are there with third term c? (You will use the same idea as in the proof of Corollary 19, but because of the requirement of primitivity, and the assumption that all terms are positive, the answer will be different. In fact, you can first figure out, for an arbitrary integer n whose prime factors are all $\equiv 1 \pmod 4$, how many ways there are of writing n as the sum of the squares of two positive integers, and then apply this to $n = c^2$.)

§8.3, ‘‘**Exercise 14**’’: Though the most useful generalizations of the concept of Unique Factorization Domain involve unique factorization of certain sorts of ideals, rather than of ring elements (p.286, second paragraph of (5); cf. p.764, Theorem 15(5)), it is also instructive to look at conditions on factorization of ring elements that generalize the condition of being a UFD. Of the seven conditions (i)-(vii) listed below, it is in general not hard to see that each implies the next. (The implication (iv)⇒(v) takes some thought, but I won’t ask you to prove it here.) In this exercise we will show that none of these implications is reversible.

Let R be, in each case, an integral domain. The seven conditions are:

(i) R is a unique factorization domain.

(ii) Every nonzero nonunit r of R can be factored into irreducibles, and all such factorizations of a given element r involve the same number of factors.

(iii) For every nonzero nonunit r of R, there is an upper bound on the number of factors in factorizations of r into nonunit factors.

(iv) Every chain of factorizations of a nonzero nonunit $r_1 \in R$ into nonunit factors of the form

$$r_1 \;=\; r_2 s_1 \;=\; r_3 s_2 s_1 \;=\; \ldots \;=\; r_n s_{n-1} \ldots s_2 s_1 \;=\; \ldots$$

(where $r_1 = r_2 s_1$, $r_2 = r_3 s_2$, ..., $r_n = r_{n+1} s_n$, ...) eventually terminates (has only finitely many steps). Equivalently: R has no infinite strictly increasing sequence of principal ideals $(r_1) \subset (r_2) \subset \ldots \subset (r_n) \subset \ldots$.

(v) Every nonzero nonunit of R can be written as a product of irreducibles.

(vi) Every nonzero nonunit of R is divisible by an irreducible.

(vii) R is (merely) an integral domain.

Here are the examples establishing that each condition is satisfied by a larger set of rings than the one before. In each case, let F be a field.

(a) If F is not of characteristic 2, show that (ii) but not (i) holds for the subring $R \subseteq F[x,y]$ consisting of polynomials in which all monomials that occur have even degrees; in other words, the subring generated by F and the elements x^2, xy and y^2.

(Hint: Let α be the automorphism of $F[x,y]$ that fixes all elements of F, sends x to $-x$, and sends y to $-y$. Verify that R consists of all elements fixed under F. Call these the ‘‘even’’ elements of $F[x,y]$, and call an element f ‘‘odd’’ if $\alpha(f) = -f$. Show that an element of R is irreducible if and only if either it is irreducible in $F[x,y]$, or it is the product of two odd irreducible elements of $F[x,y]$, or it is an associate of an element of the form $f\,\alpha(f)$, where f is an irreducible element of $F[x,y]$ that is neither even nor odd. Given an element of R and its factorization into irreducibles in $F[x,y]$, you should now be able to describe all its factorizations into irreducibles in R, and in particular, how many factors are involved.)

(b) Show that an example satisfying (iii) but not (ii) is the ring $F[x^2, x^3]$ defined in §8.1, ‘‘Exercise 13’’, sentence preceding part (c).

In the part (c) below, and also in part (f), we will use the following construction. Let us take a group isomorphic to the additive group of rational numbers, but written multiplicatively, letting the elements to be symbols x^q, where q ranges over $\mathbb{Q}$, with multiplication given by $x^q x^r = x^{q+r}$. (We may write x^0 as 1 and x^1 as x.) Calling this group $x^{\mathbb{Q}}$, we form the group ring $F x^{\mathbb{Q}}$. (The book defines the group ring FG only for a finite group G, but the same construction is possible for any group. In that construction, rather than using formal F-linear combinations of *all* group elements, one takes such combinations in which only finitely many group elements appear, just as a polynomial ring consists of polynomials in which only finitely many monomials occur.) In each of our examples, we will then take some subset S of $\mathbb{Q}$ containing 0 and closed under addition, and we will let $R = Fx^S$, the subring of $Fx^{\mathbb{Q}}$ consisting of elements in which only monomials x^r with $r \in S$ occur. (Intuitively, ''polynomials in rational powers of x, with exponents lying in S''.)

(c) Let S be the set of nonnegative rational numbers consisting of 0, and all sums of finitely many reciprocals of primes. (E.g., S includes $1/2$, $2/3 = 1/3 + 1/3$, $5/6 = 1/2 + 1/3$ and $1 = 1/2 + 1/2$; but not $1/6$.)

Show that the ring $R = Fx^S \subseteq Fx^{\mathbb{Q}}$ satisfies (iv) but not (iii).

(Suggestion: For $s_1, \dots, s_k \in S$, let $P(s_1, \dots, s_k)$ denote the set of all primes dividing the denominators of the lowest-terms expressions of any of $s_1, \dots, s_k$. If $s_1 \in S$ is equal to a sum of elements $s_2 + \dots + s_n$ $(s_2, \dots, s_n \in S)$, prove the bound $|P(s_1, \dots, s_n)| \leq |P(s_1)| + s_1$. Now given $(r_1) \subset (r_2) \subset \dots$ as in (iv), apply the above result to $\deg(r_1), \deg(r_2), \dots \in S$, and conclude that for some k, the set of primes $P(\deg(r_1), \dots, \deg(r_k))$ reaches a maximum size. Letting q be the product of the primes in that maximum set, the numbers $\deg(r_1) > \dots > \deg(r_n) > \dots$ will be nonnegative rationals all of which can be written with denominator q; deduce that the sequence terminates, proving (iv). On the other hand, to show (iii) fails, take $r = x$.)

(d) Show that a ring R satisfying (v) but not (iv) can be described as follows: Start with the field $F(u, v, x, y)$ of rational functions in four indeterminates, and let R be the subring generated by the elements of F, all elements of the forms $u^n x$ and $v^n y$ for integers n (positive and negative), and the element uv.

(Suggestion: If $r \in R$ involves x and/or y, i.e., is not just a polynomial in the element uv, consider factorizations of r into factors each of which likewise involves at least one of x and/or y. Show that for any r, the number of factors in such factorizations is bounded, and take such a factorization of r into the largest possible number of such terms. Show that none of the factors has *both* x and y appearing in all of its monomials – namely, that if one did, one could pull out a factor $u^n x$ for some n. Then show that each factor, if not itself irreducible, can be written as the product of some polynomial in uv, and an irreducible element.)

(e) Let $\mathbb{Z}[\mathbb{Q}x]$ denote the subring of $\mathbb{Q}[x]$ consisting of all elements with integer constant term. Show that this ring satisfies (vi) but not (v).

(f) Letting $\mathbb{Q}^{\geq 0}$ denote the set of nonnegative rational numbers, show that $R = Fx^{\mathbb{Q}\geq 0}$, the corresponding subring of $Fx^{\mathbb{Q}}$, satisfies (vii) but not (vi).

§8.3, ''**Exercise 15**'': Let R be an integral domain. Show that R is a unique factorization domain if and only if every nonzero nonunit of R is a product of prime elements.

§9.3, ''**Exercise 6**'': Suppose R is an integral domain, and F its field of fractions. Suppose $a(x) \in R[x]$ is monic, and $b(x)$ is any member of $F[x]$ such that $a(x)\,b(x) \in R[x]$. Show that $b(x) \in R[x]$.

(Since R is not assumed a unique factorization domain, you cannot use Gauss's Lemma. Suggested approach: Show that for any $a(x)$ and $c(x)$ in $R[x]$ with $a(x)$ monic, the result of ‘‘division with remainder of $c(x)$ by $a(x)$ in $F[x]$’’, as in the Euclidean algorithm for $F[x]$, gives quotient and remainder again in $R[x]$. Apply this in the above situation, with $c(x) = a(x)\,b(x)$.)

§9.4, ‘‘**Exercise 21**’’: (Variant of Eisenstein’s criterion.) Let R be a commutative ring, P a prime ideal of R, and $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ a polynomial over R such that $a_n \notin P$, $a_{n-1}, a_{n-2}, \ldots, a_0 \in P$, and $a_1 \notin P^2$. (These assumptions are as in Eisenstein’s criterion, p.309, except that I have weakened ‘‘$a_n = 1$’’ to ‘‘$a_n \notin P$’’, as could also have been done there, and more significantly, have changed $a_0 \notin P^2$ to $a_1 \notin P^2$.)

Show that either $f(x)$ is irreducible, or it has a factorization $f(x) = (x-a)\,g(x)$, where $a \in P$, and $g(x) \in R[x]$ is irreducible.

§13.1, ‘‘**Exercise 9**’’: In any commutative ring R with 1, let us define a *Fibonacci-like sequence* to mean a sequence of elements $(r_n)_{n\in\mathbb{Z}}$ such that for all $n\in\mathbb{Z}$, $r_{n+2} = r_{n+1} + r_n$.

Let us also define *the* Fibonacci sequence in R to mean the Fibonacci-like sequence $(f_n^{(R)})_{n\in\mathbb{Z}}$ such that $f_0^{(R)} = 0$ and $f_1^{(R)} = 1$. This is clearly the image of the ordinary sequence of Fibonacci numbers f_n in $\mathbb{Z}$ under the homomorphism $\mathbb{Z} \to R$ taking $1\in\mathbb{Z}$ to $1\in R$.

You may have seen Fibonacci numbers f_n defined only for nonnegative n. If so, a little scribbling should convince you that one can also use the formula $f_{n+2} = f_{n+1} + f_n$ to work back from the values at 0 and 1 to get f_n for negative values of n as well. You may, in fact, take for granted below that a Fibonacci-like sequence $(f_n^{(R)})_{n\in\mathbb{Z}}$ is uniquely determined by specifying the values of r_0 and r_1.

In this exercise, we shall describe the Fibonacci sequences of certain finite fields, and deduce from this some properties of the Fibonacci sequence in $\mathbb{Z}$.

(a) Show that if a commutative ring R has an element τ satisfying $\tau^2 = \tau + 1$, then the element $\tau' = 1-\tau$ satisfies the same equation, $\tau'^2 = \tau' + 1$, these two elements are both invertible, and the sequences $(\tau^n)_{n\in\mathbb{Z}}$ and $(\tau'^n)_{n\in\mathbb{Z}}$ in R are both Fibonacci-like sequences.

(b) Deduce that in the above situation, if R is a field F, and $\tau' \neq \tau$, then *the* Fibonacci sequence in F is given by the formula

$$f_n^{(F)} \;=\; (\tau^n - \tau'^n)/(\tau - \tau').$$

Deduce from this that if, moreover, τ/τ' has finite order d in $F^\times$, then $\{n \mid f_n^{(R)} = 0\} = d\mathbb{Z}$.

(c) Show that if F is a field in which 5 is a nonzero square and $2 \neq 0$, then there exist distinct τ, τ' as above, namely, $(1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$ (where $\sqrt{5}$ denotes one of the two square roots of 5 in F).

(d) Deduce that if $p\in\mathbb{Z}$ is an odd prime such that in $\mathbb{F}_p$, 5 is a nonzero square, then there exists some positive integer $d \mid p-1$ such that $\{n \mid f_n$ is divisible by $p\} = d\mathbb{Z}$.

To get information about $\{n \mid f_n$ is divisible by $p\}$ when 5 does not have a square root in $\mathbb{F}_p$, we need to use an extension of the field $\mathbb{F}_p$.

(e) Show that if 5 is not a square in $\mathbb{F}_p$ (which in particular excludes the cases $p = 2, 5$), then there exists an extension field F of $\mathbb{F}_p$, having p^2 elements, in which 5 is a square.

(f) Deduce that if 5 is not a square in $\mathbb{F}_p$, then there exists an integer $d \mid p^2-1$ such that $\{n \mid f_n$ is divisible by $p\} = d\mathbb{Z}$.

Further notes: The above arguments, between them, apply to divisibility of Fibonacci numbers by all primes p except 2 and 5. For $p = 2$ one finds that even though 5 has a square root, there is no $\tau \in \mathbb{F}_2$ satisfying $\tau^2 = \tau + 1$ (the formula $(1+\sqrt{5})/2$ obviously won't work), hence one can extend $\mathbb{F}_2$ as in (e) and (f) above, and conclude that there is a $d \mid 2^2 - 1$ as in (f). This turns out to be exactly $2^3 - 1 = 3$: f_n is even if and only if n is a multiple of 3.

For $p = 5$, we get $\tau = \tau' = (1+\sqrt{0})/2 = 1/2 = 3$, so again the above analysis does not apply; indeed, $x^2 - x - 1$ factors as $(x-3)^2$. So the above formula for $f_n^{(\mathbb{F}_p)}$ fails. In this case, there is a ''d'' as in the above results, namely 5, though this is not the multiplicative order of any element in a field of characteristic 5.

Returning to the case of (e) and (f) above, one can get in that situation a stronger result than the one we proved; namely, that d in fact divides $p+1$. The argument properly belongs to Chapter 14, but I will sketch it, using only Chapter 13 material, in the remaining points.

(g) Under the assumptions of parts (e) and (f) above, show that if we write elements of F in the form $a + b\sqrt{5}$, with $a, b \in \mathbb{F}_p$, then the map $\alpha\colon a + b\sqrt{5} \mapsto a - b\sqrt{5}$ is an automorphism of F.

(h) Show that the function N defined by $N(r) = r\,\alpha(r)$ yields a group homomorphism $F^\times \to (\mathbb{F}_p)^\times$, whose image contains all elements that are squares in $(\mathbb{F}_p)^\times$ and also 5, which is not a square.

(i) Deduce with the help of Proposition 9.6 (p.314) that $N(F^\times)$ is all of $(\mathbb{F}_p)^\times$, and hence determine the order of the kernel of the homomorphism N of multiplicative groups.

(j) Show that τ/τ' lies in the kernel of the above homomorphism. (Hint: $\tau' = \alpha(\tau)$.) Deduce that the d of part (e) indeed divides $p+1$.

With a further tool (the ''law of quadratic reciprocity''), studied in Math 115 (and sometimes in 250A), one can determine *which* primes p have the property that 5 is a square in $\mathbb{F}_p$ (just as we determined in §8.3 which primes have the property that -1 is a square in $\mathbb{F}_p$).

§13.1, ''**Exercise 10**'': Let F be a field, $F[t]$ a polynomial ring in one indeterminate t over F, and $F(t)$ its field of fractions. As noted in Example (7) on p.516, the polynomial $x^2 - t$ is irreducible in $F(t)[x]$, so that one can construct an extension field $F(t)(t^{1/2})$ by adjoining to $F(t)$ a root of that polynomial.

Show that $F(t) \cong F(t)(t^{1/2})$ as fields, by an isomorphism sending t to $t^{1/2}$.

(You may use the ''universal property of polynomial rings'' that I discussed in class: That given any homomorphism of commutative rings with unit, $\varphi\colon R \to S$, and any element $s \in S$, there is a unique homomorphism $\psi\colon R[x] \to S$ which agrees with φ on R, and takes x to s.)

§13.2, ''**Exercise 23**'': Let p be a prime, let $\alpha \in \mathbb{R}$ be the real cube root of p, and let $\beta \in \mathbb{C}$ be a non-real cube root of p. If in the diagram on p.529 we take $F = \mathbb{Q}$, $K_1 = \mathbb{Q}(\alpha)$, $K_2 = \mathbb{Q}(\beta)$, find the four degrees shown in that diagram.

Appendix I.2, ''**Exercise 5**'': Let G be a group.

(i) If S is a generating set S for G, show that a subgroup $H \leq G$ is a proper subgroup of G if and only if $S \cap H$ is a proper subset of S.

In the remaining parts, we shall consider the set of subgroups of G as partially ordered by the relation ''is a subgroup of''. Thus, the definitions on p.908 are applicable with that interpretation of ''$\leq$''.

(ii) Show that if B is a *chain* of subgroups of G, then $\bigcup_{H\in B} H$ is a subgroup of G.

(iii) For B as in (ii), show that if G is *finitely* generated, and all members of B are proper subgroups of G, then $\bigcup_{H\in B} H$ is a proper subgroup of G. (Hint: Use part (i).)

(iv) Deduce that if G is finitely generated, then every proper subgroup $H \leq G$ is contained in a *maximal* proper subgroup M of G. (I.e., a proper subgroup M of G such that no subgroup of G strictly containing M is proper. Hint: Part (iii) makes it possible to apply Zorn's Lemma to the partially ordered set of all proper subgroups of G containing H. Note why a maximal element of that set will be maximal among proper subgroups of G.)

The above is the main result of this exercise. We end with two related examples.

(v) For any proper nonzero subgroup $n\mathbb{Z} < \mathbb{Z}$ $(n>1)$, describe explicitly, in terms of the properties of the integer n, what the maximal proper subgroups of $\mathbb{Z}$ containing $n\mathbb{Z}$ are. (Zorn's Lemma does not give an explicit description, only existence; so this part is not based on that lemma.) No proof needed.

(vi) Show, in contrast to part (iv), that the group $\mathbb{Z}$ has no *minimal nonzero* subgroup. (''Minimal'' is defined like ''maximal'', but with the inequality reversed.)

(Further remarks: A different sort of contrast to the result of part (iv) is shown in §6.1, Exercise 16, namely that the *non-finitely-generated* group $\mathbb{Q}$ has *no* maximal proper subgroups. A related example is the group $\mathbb{Q}/\mathbb{Z}$, where there are again no maximal proper subgroups, but now every nonzero subgroup does contain a minimal nonzero subgroup – the opposite of the properties of $\mathbb{Z}$ in both respects.)

Appendix I.2, ''**Exercise 6**'': Show that if a group G has a non-finitely-generated subgroup, then the set of non-finitely-generated subgroups of G has a maximal member.

Appendix I.2, ''**Exercise 7**'': Let A be a nonempty set. Since partial orderings, as defined on p.908, are binary operations, and binary operations, as noted on p.3, can be regarded as subsets of $A\times A$, we can partially order the set of partial orderings on A by the inclusion relation among these subsets. We shall denote various partial orderings on A by $\leq_1$, $\leq_2$, etc., and write the inclusion relation among these by writing $(\leq_1) \subseteq (\leq_2)$, etc..

(i) Show that the maximal members of the set of partial orderings on A are the total orderings. (It is not hard to show that total orderings are maximal; the hard part is the converse. The idea is to show that if under a given partial ordering $\leq_1$, neither x nor y lies above the other, then we can enlarge $\leq_1$ to a relation $\leq_2$ such that $x \leq_2 y$, and which still satisfies the definition of a partial ordering.)

(ii) Deduce that every partial ordering on A is contained in (or, as one often says, can be strengthened to) a total ordering.