Exercises supplementing those in Beachy and Blair's *Abstract Algebra*, 3rd Edition

Most of the items in this collection are exercises that I have put on homework sheets when teaching from this text, supplementing those in the book. Some I included in the assignments the students were to hand in; most I described as for ''students interested in further interesting and/or more challenging problems'' to think about. I've also put in a few that I thought of after the course, or used on exams during the course.

Some of these exercises have many parts. Often I have assigned only the first few, the later ones being either more difficult, or too lengthy to include in an assignment that already had many exercises.

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 one of my exercises as a variant or an ''additional part'' of one of in the text. In all cases, the numbers of my exercises are shown in quotation marks, to distinguish them from the exercises in the text.

George M. Bergman
gbergman@math.berkeley.edu
17 May, 2007

– = ≡ ≡ = –

§1.2, ''**Exercise 26**'': Let a, b and c be positive integers. Using the notation $(\ ,\ )$ for g.c.d. and $[\ ,\ ]$ for l.c.m., show that $(a,[b,c]) = [(a,b),(a,c)]$, and that $[a,(b,c)] = ([a,b],[a,c])$.

§1.2, ''**Exercise 27**'': (Extension of §1.2, Exercise 13.)

(a) Let a, b, c be nonzero integers. Prove that $(a,b,c) = 1$ if and only if $(a+b+c,\ ab+ac+bc,\ abc) = 1$.

(b) State and prove a generalization of the results of part (a) above (concerning three nonzero integers) and Exercise 13 (concerning two nonzero integers) to the case of n nonzero integers $a_1, \ldots, a_n$.

(Suggestion: For $i = 1, \ldots, n$, let s_i denote the sum of all products formed using exactly i of the factors $a_1, \ldots, a_n$. Thus, for $n = 2$, s_1 and s_2 are $a_1 + a_2$ and $a_1 a_2$, corresponding to the terms occurring in Exercise 13, while for $n = 3$ we get the terms occurring in part (a) above.)

§1.3, ''**Exercise 31**'': Prove the following converse to the second assertion of Proposition 1.3.3(b):

Suppose n is a positive integer, and a an integer such that for all integers b and c, if $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$. Then $(a,n) = 1$.

§2.1, ''**Exercise 9(f-h)**'': Same instructions as for §2.1 Exercise 9(a-e) in the text, for the cases:

(f) $f: \mathbf{Z}_2 \to \mathbf{Z}_4$ given by $f([x]_2) = [x^2]_4$.

(g) $g: \mathbf{Z}_4 \to \mathbf{Z}_2$ given by $f([x]_4) = [x(x-1)/2]_2$.

And finally, for arbitrary $n > 0$ and $a \in \mathbf{Z}$ that satisfy $(a,n) = 1$:

(h) $h: \mathbf{Z}_{\varphi(n)} \to \mathbf{Z}_n$ given by $h([x]_{\varphi(n)}) = [a^x]_n$, where x ranges over all *nonnegative* integers.

§2.2, ''**Exercise 13**'': (a) Suppose X is a set, $\sim$ is an equivalence relation on X, and $f: X \to Y$ is a function from X to some set Y. Let $\sim_f$ be defined as in Example 2.2.2, p.64. Recall that by definition, $\sim$ and $\sim_f$ are both subsets of $X \times X$.

Show that the following conditions are equivalent (i.e., that each implies the other):

(i) The rule $g([x]_\sim) = f(x)$ yields a well-defined function $g: X/\sim\ \to Y$.

(ii) $\sim$ is a subset of $\sim_f$.

(b) Suppose X is a set, and $\sim_1$ and $\sim_2$ are equivalence relations on X. Deduce using part (a) that the following conditions are equivalent:

(i) The rule $f([x]_{\sim_1}) = [x]_{\sim_2}$ yields a well-defined function $f: X/{\sim_1} \to X/{\sim_2}$.

(ii) $\sim_1$ is a subset of $\sim_2$.

§2.2, ‘‘**Exercise 14**’’: 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.

§2.3, ‘‘**Exercise 17**’’: This exercise was suggested by a student’s question, whether there are any special conditions under which the composite of two cycles is a cycle.

Let n be a positive integer, and let $\sigma = (a_1, \ldots, a_s)$, $\tau = (b_1, \ldots, b_t)$ 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. (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 $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ 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 $a_1, \ldots, a_r$, and that b_j is not the first or the last term in the list $b_1, \ldots, b_s$. The cases where one or both are first or last in their lists really work the same way, but some of the expressions like ''$a_1, \ldots, a_{i-1}$'' that come up in your formula may then be empty.) What is the order of this cycle?

The next case, where $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ 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 $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ 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 $(a_1, \ldots, a_s)$ and $(b_1, \ldots, b_t)$ 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.)

§3.1, ''**Exercise 18′**'': This exercise will lead you through a careful derivation of the result that $a^s a^t = a^{s+t}$ for an element a of a group G and integers s and t, which the text asks for in Exercise 18 of this section without suggesting a method.

We will start with a version of the principle of mathematical induction that will be useful at our final step, then do the key group-theoretic calculations, and finally bring these two ideas together to get the desired result.

(a) Suppose S is a nonempty set of integers, such that for every $s \in S$ we also have $s+1 \in S$ and $s-1 \in S$. Show that $S = \mathbf{Z}$.

For the remaining parts of this exercise, G will be a group, which we will write multiplicatively, and a will be some element of G, whose inverse we shall temporarily write $\tilde{a}$. We shall consider the powers of a to be defined by the formulas

$$a^0 = e; \qquad a^{m+1} = a\,a^m \text{ for } m \geq 0; \qquad a^{m-1} = \tilde{a}\,a^m \text{ for } m \leq 0.$$

We see that for $m \geq 0$, this definition of a^m is essentially the same as that in the book.

(b) Show that the above definition of a^m also gives the same element as the definition in the book when $m < 0$. (Suggestion: Let $m = -n$ and use induction on n.)

This shows in particular that what the above definition names a^{-1} is the inverse $\tilde{a}$ of a; so from now on we will use the familiar notation a^{-1} rather than the temporary notation $\tilde{a}$.

The next part is the one where you will have to work case-by-case; but since there is only one integer variable involved, there are not too many cases.

(c) Show that for *every* integer m, one has $a\,a^m = a^{m+1}$, and $a^{-1}a^m = a^{m-1}$.

Having proved the above results, it is easy to complete the proof. Let S denote the set of integers s such that $a^s a^t = a^{s+t}$ for all integers t; in symbols

$$S = \{s \in \mathbf{Z} \mid (\forall\ t \in \mathbf{Z})\ \ a^s a^t = a^{s+t}\}.$$

(d) Show that $0 \in S$, and that for all $s \in S$ one also has $s+1 \in S$ and $s-1 \in S$. (Suggestion: Use (c) and associativity.)

(e) Deduce that $$(\forall\ s \in \mathbf{Z})\ (\forall\ t \in \mathbf{Z})\ \ a^s a^t = a^{s+t}.$$

§3.1, ‘‘**Exercise 19′**’’: Assuming parts (a) and (e) of ‘‘§3.1, Exercise 8′’’ above, prove that for all integers s and t one has $(a^t)^s = a^{ts}$. (Suggestion: This time let $S = \{s \in \mathbf{Z} \mid (\forall\ t \in \mathbf{Z})\ (a^t)^s = a^{ts}\}$.)

§3.3, ‘‘**Exercise 19**’’: If m, n are nonzero integers, regarded as members of the group $\mathbf{Z}$, show that $\langle \{m, n\} \rangle$ is the cyclic subgroup of G generated by $\gcd(m, n)$. (For the notation $\langle \ldots \rangle$, see Definition 3.3.8. Incidentally, an expression like $\langle \{m, n\} \rangle$ is often abbreviated to $\langle m, n \rangle$.)

§3.3, ‘‘**Exercise 20**’’: (a) Show that in S_4, $\langle (1,2,3,4), (1,2) \rangle$ is the whole group S_4.

(b) Show that in S_4, $\langle (1,2,3,4), (1,3) \rangle$ is the subgroup whose elements are listed at the top of Figure 3.6.1, p.145. You do not have to have read §3.6 to do this exercise; you may take as given that the elements listed in that figure do form a subgroup of S_4.

(Suggestion: Do part (b) first, showing that $\langle (1,2,3,4), (1,3) \rangle$ must be contained in the subgroup of Figure 3.6.1, and that by Lagrange’s Theorem there can be nothing strictly between $\langle (1,2,3,4) \rangle$ and that subgroup. Then do (a) by computing $(1,2)(1,2,3,4)^2(1,2)$, using an argument like that used in (b) to deduce that $\langle (1,2,3,4), (1,2) \rangle$ must contain the group of Figure 3.6.1, and then another application of Lagrange’s Theorem to show it must be all of S_4.)

§3.4, ‘‘**Exercise 29**’’: 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 one-to-one and onto map $\varphi\colon G_1 \to G_2$ 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 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 $[a, b, c] = a b^{-1} c$?

§3.6, ‘‘**Exercise 28**’’: Let n be a positive integer, and let us say an element $\sigma \in S_n$ ‘‘fixes’’ $i \in \{1, \ldots, n\}$ if $\sigma(i) = i$, that it ‘‘moves’’ i if $\sigma(i) \neq i$, that σ and τ ‘‘agree’’ on i if $\sigma(i) = \tau(i)$, and that they ‘‘differ on i’’ otherwise. The idea of this exercise is that if σ and τ agree on ‘‘most’’ elements, then $\sigma\tau^{-1}$ is a ‘‘small’’ permutation, i.e., fixes most elements. We begin with two examples.

(a) Let $3 \leq m \leq n$, let $\sigma = (1, 2, \ldots, m-1)$ and let $\tau = (1, 2, \ldots, m)$. Calculate $\sigma\tau^{-1}$, showing your reasoning.

(b) Let $3 \leq m \leq n-2$, let $\sigma = (1, 2, \ldots, m-1)(m, \ldots, n)$ and $\tau = (1, 2, \ldots, m)(m+1, \ldots, n)$. Calculate $\sigma\tau^{-1}$, showing your reasoning.

(c) Suppose $\sigma, \tau \in S_n$ differ on exactly m elements. Show that $\sigma\tau^{-1}$ moves exactly m elements.

(d) Suppose $\sigma, \tau \in S_n$, and that τ moves exactly k elements. Show that $\tau\sigma\tau^{-1}$ differs from σ on at most $2k$ elements. Deduce that $\tau\sigma\tau^{-1}\sigma^{-1}$ moves at most $2k$ elements.

§3.6, ‘‘**Exercise 29**’’: (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 $\sigma = \rho^2$).

(c) Is it true that for every n, the elements of A_n are precisely the permutations that are squares in S_n? If this is not true in general, for which n is it true?

§3.6, ‘‘**Exercise 30**’’: Recall from p.146 that if n is an integer ≥ 3, every element of the group D_n of symmetries of a regular n-gon can be written uniquely in the form $a^i b^j$ where $0 \leq i < n$, $0 \leq j < 2$.

(a) In the group D_7, express the following elements in the form described:

(i) ba^3, (ii) $b^4 a^{-1}$, (iii) $(a^2 b)^2$, (iv) $(ab)^{-1}$.

(b) Let n be any integer ≥ 3. Determine the order of every element $a^i b^j$ $(0 \leq i < n,\ 0 \leq j < 2)$ of D_n.

(In doing so, you may divide into cases according to the values of i and/or j. However, try to simplify your argument and your answer as much as possible, e.g., by combining cases that you may have initially considered separately, if this is possible. Proposition 3.5.3, in which a single formula expresses the order of an element a^m in a cyclic group $\langle a \rangle$ of order n, is useful to keep in mind.)

§3.7, ‘‘**Exercise 32**’’: Suppose G, H and K are groups, and $\varphi: G \to H$, $\psi: G \to K$ are homomorphisms such that $\ker(\varphi) = \ker(\psi)$. Show that $\varphi(G) \cong \psi(G)$.

§3.8, ‘‘**Exercise 5′**’’: Let G be a group and H a subgroup. We wish to show that the number of left cosets of H in G is equal to the number of right cosets of H in G, or – to put this in a form that makes sense when there are infinitely many cosets – that there is a one-to-one correspondence between the two sorts of cosets. The first part of this exercise will show that the naive way to attempt to define such a correspondence does not work in general. The second part shows a way that does work.

(a) Show by example that one does not in general get a well-defined map f from the left cosets of H in G to the right cosets of H in G by the rule $f(aH) = Ha$.

(b) Show that the rule $f(aH) = Ha^{-1}$ does give a well-defined map f from the left to right cosets

(c) Show that the map constructed in part (b) is one-to-one and onto.

Suggestion for (a): If H is normal, a result in the book implies that the map f above is well-defined, so you need to use an example of a non-normal H. Suggestion for (c): The easiest way to show the map is one-to-one and into is to construct an inverse map.

§3.8, ‘‘**Exercise 29**’’: This exercise will give what I think is a more natural version of the proof of Proposition 3.8.4.

Suppose G is a group, and H a subgroup of G. Below, a, a_1, a_2, b, b_1, b_2 will denote arbitrary elements of G.

(a) Show that if H is normal in G, and if $a_1 H = a_2 H$, then $a_1 b H = a_2 b H$. (Do not assume Proposition 3.8.4 or any result proven after it, since this is part of a proof of that proposition.)

(b) Show, regardless of whether H is normal, that if $b_1 H = b_2 H$ then $a b_1 H = a b_2 H$.

(c) Deduce from (a) and (b) that if H is normal in G, and $a_1 H = a_2 H$ and $b_1 H = b_2 H$, then $a_1 b_1 H = a_2 b_2 H$.

§4.1, ''**Exercise 25**'': This exercise generalizes Exercises 13 and 14 of §4.1. Parts (a) and (b) may be regarded as ''warm-ups'' for part (c). So you might work out those two on scrap paper, then try to do (c), and if you succeed in answering (c), write up the results of (a) and (b) as consequences of that general result.

(a) For what rational numbers r is it true that the set of matrices $\{ \begin{bmatrix} a & b \\ rb & a \end{bmatrix} \mid a, b \in \mathbf{Q} \}$ forms a field under the operations of matrix addition and multiplication?

(b) Same question for real numbers r and the set $\{ \begin{bmatrix} a & b \\ rb & a \end{bmatrix} \mid a, b \in \mathbf{R} \}$.

(c) Same question for elements r of an arbitrary field F, and the set $\{ \begin{bmatrix} a & b \\ rb & a \end{bmatrix} \mid a, b \in F \}$.

§4.4, ''**Exercise 21**'': Suppose $f(x),\ g(x) \in \mathbf{Q}[x]$. Using the division algorithm, let us write $f(x) = q(x)g(x) + r(x)$ with $q(x),\ r(x) \in \mathbf{Q}[x]$, and either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$.

(a) Show that if $f(x),\ g(x) \in \mathbf{Z}[x]$, and $g(x)$ is monic, then $q(x),\ r(x) \in \mathbf{Z}[x]$. (Suggestion: If $q(x) \notin \mathbf{Z}[x]$, look at the highest-degree term of $q(x)$ whose coefficient is not in $\mathbf{Z}$.)

(b) Show by example that if we merely assume that $f(x),\ g(x) \in \mathbf{Z}[x]$, but not that $g(x)$ is monic, then the conclusion of (a) can fail.

§4.4, ''**Exercise 22**'': (Variant of Eisenstein's criterion.)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ be a polynomial with integer coefficients, and p a prime number. Suppose that $a_n \not\equiv 0 \pmod p$, $a_{n-1} \equiv a_{n-2} \equiv \ldots \equiv a_0 \pmod p$, and $a_1 \not\equiv 0 \pmod{p^2}$. (These assumptions are the same as for Eisenstein's criterion, p.214, except that I have replaced ''$a_0 \not\equiv 0 \pmod{p^2}$'' with ''$a_1 \not\equiv 0 \pmod{p^2}$''.)

Show that either $f(x)$ is irreducible, or it has a factorization $f(x) = (x-n)g(x)$, where $n \in p\mathbf{Z}$, and $g(x) \in \mathbf{Z}[x]$ is irreducible.

§5.1, ''**Exercise 23**'': (Continuation of §5.1 Exercise 4(a).)

(a) Show that if $m + n\sqrt{2}$ is a unit in $\mathbf{Z}[\sqrt{2}]$, then by multiplying either by $1+\sqrt{2}$ or its inverse, one can ''usually'' get a unit $m' + n'\sqrt{2}$ of this ring with $|m'|+|n'| < |m|+|n|$. Here by ''usually'' I mean ''except for certain cases involving small values of $|m|+|n|$'', which you should determine explicitly.

(b) From the result of (a), determine explicitly the group of units of $\mathbf{Z}[\sqrt{2}]$.

§5.1, ''**Exercise 24**'': (A different continuation of §5.1 Exercise 4(a).)

It is not hard to see that if m and n are positive integers such that $m + n\sqrt{2}$ is a unit in $\mathbf{Z}[\sqrt{2}]$, then by multiplying by $1+\sqrt{2}$, we get a unit $m' + n'\sqrt{2}$ of this ring with $m' + n' > m + n$.

(a) Derive from this a rule which, taking any pair of nonnegative integers m and n satisfying $|m^2 - 2n^2| = 1$, gives a pair of nonnegative integers m' and n' satisfying $|m'^2 - 2n'^2| = 1$, with $m' + n' > m + n$. Check by direct computation on m and n (without reference to the ring $\mathbf{Z}[\sqrt{2}]$) that your rule has the above properties.

(b) Show that if m and n are positive integers satisfying $|m^2 - 2n^2| = 1$, then m/n is close to $\sqrt{2}$, where you should give a precise meaning to ''close'', in the form of a lower bound on $|m/n - \sqrt{2}|$ in terms of m and/or n.

(c) Use this method to find a rational number m/n with m and n integers less than 20, which approximates $\sqrt{2}$ to within 0.01.

§5.3, ‘‘**Exercise 27**’’: Let a and b be relatively prime integers, and let $\varphi\colon\ \mathbf{Z} \to \mathbf{Z}[i]/\langle a+bi\rangle$ be the map that takes each integer m to the congruence class of m modulo $\langle a+bi\rangle$; i.e., $\varphi(m) = m+\langle a+bi\rangle$.

(a) Show that φ is onto. (Suggestion: Write down the general expression for an element of $\langle a+bi\rangle$, i.e., a multiple of $a+bi$ in $\mathbf{Z}[i]$, and show that there exists an element of that sort having the form $r+i$ with $r\in\mathbf{Z}$. Deduce that i is congruent to a member of $\mathbf{Z}$ modulo $\langle a+bi\rangle$, from this deduce that every element $m+ni$ is congruent to a member of $\mathbf{Z}$, and show that this makes φ onto.)

(b) Show that the kernel of φ is $\langle a^2+b^2\rangle$, i.e., the ideal of $\mathbf{Z}$ generated by a^2+b^2.

(c) Deduce that $\mathbf{Z}[i]/\langle a+bi\rangle \cong \mathbf{Z}/\langle a^2+b^2\rangle$ (i.e., $\mathbf{Z}_{a^2+b^2}$).

(d) On the other hand, show that if a and b are two integers that are not relatively prime, then $\mathbf{Z}[i]/\langle a+bi\rangle$ is not isomorphic to $\mathbf{Z}_n$ for any n. (Hint: If $p \mid \gcd(a,b)$, find a homomorphism of $\mathbf{Z}[i]/\langle a+bi\rangle$ onto $\mathbf{Z}[i]/\langle p\rangle$, and show that as an additive group, the latter ring is isomorphic to $\mathbf{Z}_p\times\mathbf{Z}_p$, hence not cyclic.)

§5.3, ‘‘**Exercise 28**’’: Let R be a commutative ring. As shown in §5.3 Exercise 7, the intersection of two ideals of R is again an ideal. Below, we first note a couple of variants of this statement that are not true, then show further refinements of those statements that are true.

(a) Show that if I and J are ideals of R, then $I\cup J$ is not an ideal unless either $I\subseteq J$ or $J\subseteq I$.

(b) Show that if I and J are prime ideals of R, then $I\cap J$ is not prime unless $I\subseteq J$ or $J\subseteq I$.

(c) Suppose $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ are ideals of R (i.e., that we have an ideal I_n for each natural number n, with $I_m \subseteq I_n$ whenever $m\leq n$). Show that $\bigcup_{n\in\mathbf{N}} I_n$ is an ideal, and is prime if all the I_n are prime. (For the meaning of the symbol $\bigcup_{n\in\mathbf{N}}$, see p.434. Also note on that page the meaning of $\bigcap$, used in the next part below.)

(d) Suppose, instead, that we have ideals $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n \supseteq \ldots$ in R. Show that $\bigcap_{n\in\mathbf{N}} I_n$ is an ideal, and is prime if all the I_n are prime.

In parts (c) and (d), the ideals were indexed by natural numbers because that is the kind of indexing students are most familiar with. But the results can be generalized:

A family $\{S_\lambda \mid \lambda\in\Lambda\}$ of subsets S_λ of a set X is called a *chain* if for all $\lambda,\mu\in\Lambda$, either $S_\lambda \subseteq S_\mu$ or $S_\lambda \supseteq S_\mu$.

(e) Show the if $\{I_\lambda \mid \lambda\in\Lambda\}$ is any chain of ideals of R, then both $\bigcup_{\lambda\in\Lambda} I_\lambda$ and $\bigcap_{\lambda\in\Lambda} I_\lambda$ are ideals, and that if all I_λ are prime, then both these ideals are also prime.

§5.4, ‘‘**Exercise 15**’’: (a) If R is any commutative ring, show that the intersection of all subrings of R is $\{n\cdot 1 \mid n\in\mathbf{Z}\}$.

(b) A field that is isomorphic to $\mathbf{Q}$, or is isomorphic to $\mathbf{Z}_p$ for a prime number p, is called a *prime field*. Corollary 5.4.8 says that every field has a subfield that is a prime field. Show that a field F has one and only one such subfield, and that this subfield is the intersection of all the subfields of F.

(A slightly different definition of prime subfield is given on p.295, but the above result shows it is equivalent to the above definition.)

In the next two parts you may assume the result of §5.2 Exercise 10.

(c) If R is any commutative ring and $\varphi\colon R \to R$ any homomorphism, show that $\varphi(a) = a$ for all a in the subring described in part (a) above.

(d) If F is any field, and $\varphi\colon F \to F$ any homomorphism, show that $\varphi(a) = a$ for all a in the subfield described in part (b) above.

§5.4, ‘‘**Exercise 16**’’: (a) Suppose we have a family of rings R_i, one for each natural number i, and we let $\Pi_{i\in\mathbf{N}} R_i$ denote the set of all sequences $(a_0, a_1, \ldots)$ such that $a_i \in R_i$ for each i. Show that the operations

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$
$$(a_0, a_1, \ldots)\,(b_0, b_1, \ldots) = (a_0\, b_0, a_1\, b_1, \ldots)$$

make $\Pi_{i\in\mathbf{N}} R_i$ a commutative ring. Below, we shall abbreviate $\Pi_{i\in\mathbf{N}} R_i$ to $\Pi\, R_i$.

(b) In the context of part (a), let I denote the set of elements of $\Pi\, R_i$ which have *all but finitely many components zero*; i.e.,

$$I = \{(a_0, a_1, \ldots) \mid \{i\in\mathbf{N} \mid a_i \neq 0\} \text{ is finite}\}.$$

Show that I is an ideal of $\Pi\, R_i$.

(c) Let p_0, p_1, ... be the list of all prime numbers (i.e., $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, etc.). Show that the ring $\Pi\,\mathbf{Z}_{p_i}$ has characteristic 0.

(d) For $\Pi\,\mathbf{Z}_{p_i}$ and I as in part (c), show, that for every nonzero integer n, the element $n\cdot 1 \in (\Pi\,\mathbf{Z}_{p_i})/I$ is invertible.

(e) Deduce that $(\Pi\,\mathbf{Z}_{p_i})/I$ has a subring isomorphic to the field $\mathbf{Q}$ of rational numbers.

§6.2, ‘‘**Exercise 12**’’: Let K be a field, and R a commutative ring containing K. Then we may regard R as a vector-space over K. (A special case of this is stated as Proposition 6.2.1.)

Show that if R is an integral domain and is finite-dimensional over K, then R is a field. (This is an analog of Theorem 5.1.9, with ‘‘finite-dimensional’’ in place of ‘‘finite’’.)

§7.2, ‘‘**Exercise 19**’’: Let G be a group.

Show that for any two elements $a, b\in G$ the products ab and ba are conjugate in G. Conversely, show that if $x, y\in G$ are conjugate elements, then there exist $a, b\in G$ such that $x = ab$ and $y = ba$.

§7.3, ‘‘**Exercise 15**’’: Let G be a group.

If S is a set given with an action of G on it, we shall call S a G-*set*. If S and T are G-sets, then an *isomorphism* between S and T (as G-sets) will mean a one-to-one and onto map $\varphi: S \to T$ such that for all $a\in G$ and $x\in S$ one has $\varphi(ax) = a\,\varphi(x)$. (Note that while the concept of an isomorphism 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 isomorphism of vector spaces, where one considers two vector spaces over the same field.) We shall call G-sets S and T isomorphic if there exists an isomorphism between them.

Given a G-set S and an element $x\in S$, the orbit Gx can clearly be considered a G-set (‘‘the sub-G-set of S generated by x’’). Recall also from Example 7.3.8 that for any subgroup $H \subseteq G$, the set of left cosets of H in G forms a G-set. (In that example, the authors assumed H a proper subgroup; but they only needed that for the one assertion that $S^G = \varnothing$; everything else they say there is also true in the case $H = G$. In that case, S is ‘‘uninteresting’’, but we cannot exclude it here or the result you will be asked to prove would become false.)

Show that for any G-set S, each orbit in S is isomorphic, as a G-set, to the G-set of left cosets of some subgroup $H \subseteq G$. (Hint: see Proposition 7.3.4.)

§7.3, ‘‘**Exercise 16**’’: Let G be a group. We shall use the term ‘‘G-set’’ as in the preceding exercise.

(a) If S and T are G-sets, show that the set $S\times T = \{(s, t) \mid s\in S,\ t\in T\}$ becomes a G-set if we define $a(s, t) = (as, at)$ for all $a\in G$, $(s, t)\in S\times T$.

Let us call a G-set S *transitive* if it consists of just one orbit.

(b) Show that if S and T are both finite transitive G-sets, and if g.c.d.$(|S|, |T|) = 1$, then the G-set $S\times T$ is also transitive. (Suggestion: For $s\in S$, $t\in T$, consider the relations among the indices $[G:G_s]$, $[G:G_t]$, and $[G:G_{(s,t)}]$.)

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

(d) Show that if S and T are G-sets such that the G-set $S\times T$ is transitive, then for any $t\in T$, the action of the subgroup G_t on S is transitive.

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

§7.4, ‘‘**Exercise 15**’’: In this exercise we will examine nonabelian groups of order 21, a specific example of Proposition 7.4.6(b) (p.341). For a group of order 21, the p and q of that proposition are 7 and 3 respectively, so the conditions on n in the last line of the proposition say that $n \not\equiv 1 \pmod 7$ but $n^3 \equiv 1 \pmod 7$; i.e., that $[n]_7$ is an element of order 3 in $\mathbf{Z}_7^\times$. There are two such elements, $[2]_7$ and $[4]_7$, so let us suppose we have two groups:

A group G_1 generated by nonidentity elements a_1 and b_1 satisfying

$$a_1^7 = e, \qquad b_1^3 = e, \qquad b_1 a_1 = a_1^2 b_1,$$

A group G_2 generated by nonidentity elements a_2 and b_2 satisfying

$$a_2^7 = e, \qquad b_2^3 = e, \qquad b_2 a_2 = a_2^4 b_2.$$

It is not hard to prove that in the group G_1, every element can be written uniquely as $a_1^i b_1^j$ with $0 \le i < 7$ and $0 \le j < 3$, and likewise that in the group G_2, every element can be written uniquely as $a_1^i b_1^j$ with $0 \le i < 7$ and $0 \le j < 3$; you may assume these unique-representation results in doing the parts below.

We haven't proved yet that groups G_1 and G_2 of order 21 with nonidentity elements satisfying the equations displayed above exist. In parts (a) and (b) below, you will prove facts that must be true about such groups *if* they exist. In parts (c) and (d), we will see how to construct such groups.

(a) Show that there does not exist an isomorphism $G_2 \to G_1$ taking a_2 to a_1 and b_2 to b_1.

(b) Show, however, that there does exist an isomorphism $G_2 \to G_1$. (Hint: In G_1, conjugation by b_1 acts on the Sylow 7-subgroup $\langle a_1\rangle$ by squaring every element, while in G_2, conjugation by b_2 acts on the Sylow 7-subgroup $\langle a_2\rangle$ by raising everything to the 4th power. What is the relation between the squaring and fourth-power operations?)

From Proposition 7.4.6(b), and part (b) above, one can conclude that any two nonabelian groups of order 21, if such groups exist, are isomorphic. Let us now obtain the existence of such groups.

(c) For elements $m, b\in\mathbf{Z}_7$ such that $m^3 = [1]$, let $f_{m,b}\colon \mathbf{Z}_7 \to \mathbf{Z}_7$ denote the function given by $f_{m,b}(x) = mx+b$. These functions are not group homomorphisms; for instance, in general they do not send the identity element of $\mathbf{Z}_7$ to itself. However, show that each such function is a permutation of $\mathbf{Z}_7$, and that the set of such functions, $\{f_{m,b} \mid m, b\in\mathbf{Z}_7,\ m^3 = [1]\}$, forms a subgroup G of $\mathrm{Sym}(\mathbf{Z}_7)$, of order 21.

(d) Find in the group G of part (c) nonidentity elements a_1 and b_1 satisfying the relations assumed for the generators of G_1 above, and also nonidentity elements a_2 and b_2 satisfying the relations assumed for the generators of G_2. (The four elements you find need not all be distinct.)

(Remark: This exercise is a particular case of results that can be proved with ‘‘21’’ replaced by ‘‘pq, for any primes $p < q$ with $p \mid q-1$’’. But more work is needed in proving the general statements; in particular, the explicit observations on elements of $\mathbf{Z}_7^{\times}$ having order 3 is replaced by an application of Theorem 6.5.10.)

§9.1, ‘‘**Exercise 15**’’: (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 on D has the properties stated for δ in the definition of Euclidean domain, so that D is a Euclidean domain, and hence a principal ideal domain.

The above is fairly easy. The generalization below requires considerably more 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 $v_1, \ldots, v_n : D-\{0\} \to \mathbf{N}$ 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.)

§9.2, ‘‘**Exercise 11**’’: Show that the result of §9.2, Exercise 10 becomes false if $F[x]$ is everywhere replaced by $F[w, x]$, a polynomial ring in two indeterminates over F.

§A.7, ‘‘**Exercise 1′**’’: (This is a more detailed version of the text’s Exercise 1. We assume, as in that exercise, that §3.1 has been covered; if, instead, this appendix is read before that section, then this exercise could be considered to go with §3.1 or §3.2.)

Suppose p is a prime and A is an abelian group, written additively, such that every $a \in A$ satisfies $p\,a = 0$.

(a) For every $[n] \in \mathbf{Z}_p$ and every $a \in A$, let us define $[n] \cdot a = n\,a$. (For the meaning of $n\,a$, see p.97, lines 4-6.) Show that this operation is *well-defined*. You may use the laws given in the display on p.97.

(b) Under the scalar multiplication defined in part (a), and the given additive group structure of A, show that A is a vector space over the field $\mathbf{Z}_p$. (The definition of vector space contains 10 points to be verified! However, most of them can be handled very briefly, by referring to some condition in the definition of abelian group or to part (a) above. The remaining conditions will require short computations using the above definition of scalar multiplication, the definition of the operations of the field $\mathbf{Z}_p$, and the laws of exponents.)

(c) Show, conversely, that if V is a $\mathbf{Z}_p$-vector space, then $(V, +)$ is an abelian group in which every element satisfies $p\,a = 0$.

(d) Two abelian groups are shown in Table 3.3.1, p.115. If their operations are renamed ‘‘+’’ instead of ‘‘ · ’’, then the result of (a) becomes applicable to *one* of them.

To which one, why, why not to the other, and for what prime p?

Find a basis of the resulting vector space.