EXERCISES

Naming of exercises. We will always refer to exercises in Lang by chapter, and then the exercise-number they have in that chapter, preceded by '':L''. E.g., exercise 3 at the end of Chapter II of Lang is here called ''Exercise II:L3''.

On the other hand, exercises given below are classified by the chapter and section to which they are related. For instance, exercises related to Lang's section VI.2 are numbered VI.2:1, VI.2:2, etc.. (Exercises related to Appendix 2, where Lang gives background on set theory, and to my handout on ''The Axiom of Choice, Zorn's Lemma, and all that'', to be read with that Appendix, are numbered using A2 in place of the chapter number, and are given at the end. The one exercise based on Lang's pp.ix-x, ''Logical Prerequisites'', is numbered 0:1.)

If an exercise is related to more than one section, I will list it under the last section with which it assumes familiarity (using the order of sections noted in the Introduction to this Companion when this differs from Lang's). If one exercise assumes the results of another, I indicate this with the symbol [> ...], meaning that if assigned, it should be given after the other one. In cases where one exercise refers to an idea in another, or perhaps is motivated by a result in another, but doesn't require one to assume that result, I use [cf. ...] rather than [> ...].

Exercises marked * or ¤. When I teach the course, I give homework problems, which all students are expected to do, and a few extra-credit problems, which require more original thinking.

A problem requiring ingenuity can generally be transformed into a straightforward task by adding steps to lead the student through the solution, so the same problem may be given, with modification, as an extra-credit problem one year and a regular homework question the next. Below, I have marked with an asterisk * those exercises that in *the form given here* require considerable original thinking, and could be assigned as extra-credit problems.

It sometimes also happens that an exercise seems difficult until one sees some key trick, which makes it easy. Starting with the 2002 version of these notes, I have begun using another symbol, ''¤'', to mark exercises of this sort. In general, such exercises are not good to assign as homework, but *are* good for students to think about. Until now, I have avoided including such exercises in these notes, so there will be very few until I accumulate more.

(Of course, the starred exercises also generally require some insight or key idea; but in such cases the insight is generally not as straightforward, and still takes some work to apply.)

Notes below on exercises in Lang. Some of the exercises below generalize, clarify, or correct exercises in Lang; notes on some others of Lang's exercises are given at the end of my exercises for each section. For convenience, this collection of exercises ends with an ''index'' to my commentary on Lang's exercises, both in these pages and in the body of this Companion. (But corrections that apply only to earlier printings of Lang are only noted in the Errata, as usual.)

~ ~ ~

0:1. Consider a diagram of sets and set-maps formed by taking the square diagram at the bottom of p.ix, putting a fifth set E in the center, and drawing an arrow connecting E to each of the four objects shown there. (The directions of the arrows will be specified below.)

(a) Show that if the arrow between A and E goes inward (to E) and the arrow between E and D goes outward (to D), then regardless of the direction(s) in which the arrows connecting B and E to E are drawn, commutativity of the four triangles into which those arrows divide the given square implies commutativity of the square.

(This involves four different cases depending on the directions of those arrows; but with a little thought, one can deal with these cases simultaneously.)

(b) Show that if all four arrows point in toward E, or if all four arrows point out from E, then commutativity of those four triangles does not imply commutativity of the square.

I.1:1. Let X be any set, let G be the monoid of all maps $X \to X$, where the ''multiplication'' is composition of maps, and let $H \subseteq G$ denote $\{g \in G \mid \forall x \in X,\ g^{-1}(\{x\})$ is countable$\}$. Show that H is a submonoid of G.

I.1:2. In this exercise, we shall show that there are enormous numbers of isomorphism classes of monoids of small finite cardinalities. It will be easiest to start by considering isomorphism classes of *semigroups*, that is, sets given with an associative composition, not assumed to have a unit. Then, in part (d), we will ''adjoin units''.

(a) Suppose A and B are disjoint sets, c an element not in $A \cup B$, and $f\colon A \times A \to B$ any set-map. Show that the set $S = A \cup B \cup \{c\}$ becomes a semigroup S_f if we define xy to be $f(x,y)$ if x, y both belong to A, and to be c otherwise. Assuming that A and B are finite, express the number of *distinct* (but not necessarily nonisomorphic) semigroup structures on the set $S = A \cup B \cup \{c\}$ that may be obtained by this construction using various maps f, as a function of the cardinalities $\mathrm{card}(A)$ and $\mathrm{card}(B)$.

(b) Show that given two maps $f, g\colon A \times A \to B$, any isomorphism between the semigroups S_f and S_g must carry A into A, B into B, and c to c. Deduce that among the semigroup structures described in (a), no more than $\mathrm{card}(A)!\,\mathrm{card}(B)!$ can belong to any one isomorphism class.

(c) Taking $\mathrm{card}(A) = \mathrm{card}(B) = n$, and using the estimate $n! \leq n^n$, obtain a lower bound on the number of isomorphism classes of semigroups of $2n+1$ elements.

(d) Show that if G is any semigroup, and e an element not in G, then $G \cup \{e\}$ can, in a unique manner, be made into a monoid having G as a subsemigroup and e as unit. (Note: do not confuse the uniqueness asked for here with the uniqueness of the identity element of a monoid, proved by Lang on p.3.) Show that if G and H are nonisomorphic semigroups, then $G \cup \{e\}$ and $H \cup \{e\}$ become nonisomorphic monoids.

(e) Deduce a lower bound on the number of isomorphism classes of monoids of $2n+2$ elements.

(f) Find reasonably small integers M and N such that there are at least 100 nonisomorphic monoids of M elements, and at least 10^{100} nonisomorphic monoids of N elements. (You may obtain these bounds using the estimate of point (e), or you may see whether you can get still smaller M and N by ad hoc choices of unequal values for $|A|$ and $|B|$.)

***I.2:1.** Let G be a group and S a subset. Let D be the set of all elements $x \in G$ which have the property that for every group H and every two homomorphisms $p, q\colon G \to H$ agreeing on S, we also have $p(x) = q(x)$. By the same sort of argument as we gave in the main part of these notes concerning the statement at the bottom of p.10 of Lang, we can see that D is a subgroup of G containing the subgroup generated by S. Must it equal the subgroup generated by S?

I.2:2. (a) Suppose G is a group and H, K are subgroups, and we define $HK = \{hk \mid h \in H,\ k \in K\}$. Show that HK is a subgroup of G if and only if it is closed under taking inverses.

(b) Show by example that the corresponding statement is false for 3-fold products HJK of subgroups of G.

Note on I:L44 (p.79): The assumption that A and A' be abelian is not needed. This exercise can go with §I.2.

I.2:3. (a) Suppose G and H are groups, and $a, b, c\colon G \to H$ are *set-maps*, such that for all $x \in G$,

$a(x)\,b(x) = c(x)$. Show that if *any three* of the following conditions hold, so does the fourth:

(i) a is a homomorphism.

(ii) b is a homomorphism.

(iii) c is a homomorphism.

(iv) Every element of $a(G)$ commutes with every element of $b(G)$.

(b) If one takes $H = G$, lets a and b be the identity endomorphism of G, and defines c in the unique way making part (a) applicable, what does part (a) tell us?

(c) If one takes $H = G$, lets a be the identity endomorphism of G, lets c be the trivial endomorphism (taking every element to e), and defines b in the unique way making part (a) applicable, what does part (a) tell us?

I.3:1. = I:L3 (p.75) but with the last sentence made more precise: ''Show that G/G^c is abelian, and that any homomorphism f of G into an abelian group A can be factored $f = hq$, where q is the canonical homomorphism $G \to G/G^c$, and h is a homomorphism of abelian groups, $G/G^c \to A$.'' (Recommendation: Before reading carefully the above revision, think about the version in Lang, and try to guess what it means, since you will frequently encounter such abbreviated statements.)

I.3:2. Do I:L5 (p.75). Show moreover that in this situation, H is the inverse image of the graph in question under the natural map $G\times G' \to G/N \times G'/N'$.

Deduce that if H is *any* subgroup of $G\times G'$, then there exist subgroups $K \subseteq G$, $K' \subseteq G'$ and homomorphisms f, f' from these respective subgroups into a common group L, such that

$$H = \{(k, k') \in K\times K' \mid f(k) = f'(k')\}.$$

Intuitive idea: Regard $H \subseteq G\times G'$ as a relation. If two elements $r_1, r_2 \in G$ are both ''related'' via H to a common element s_1 of G', then since H was assumed a group, $r_1 r_2^{-1}$ is related to e. One finds that the condition of ''relating to a common element'' is an equivalence relation on the group K of elements of G that relate to elements of G'. If one ''glues together'' elements of K via this equivalence relation, and does the analogous gluing job on the group K' of elements of G' that relate to at least one element of G, one gets factor groups K/N and K'/N', and the relation given by H becomes an isomorphism between these, which uniquely determines H.

(Note that for *monoids* in place of groups, the corresponding arguments fail, because of the lack of inverses; and there are submonoids of product monoids which do not arise from isomorphisms of subfactors. An example is the submonoid of $\mathbf{Z}\times\mathbf{Z}$ given by $\{(x,y) \mid x \leq y\}$.)

(Remark on Lang's use of the phrase ''identify ... as'' in I:L5 and elsewhere. This usage is not standard. There is, of course, the standard use of ''to identify X as Y'' meaning to determine that X is Y: ''He identified the specimen as belonging to an extinct species''. And there is the mathematical use of the phrase ''to identify X *with* Y'' meaning to treat X and Y as the same – sometimes by a formal construction such as dividing out by an equivalence relation; other times by ignoring an ''irrelevant'' distinction, for instance, when one identifies S_n with a subgroup of S_{n+1}. It is not clear to me whether Lang is using ''identify as'' in the sense of ''identify with'', or in a blend of the two meanings, e.g., ''we *determine* that N is isomorphic to a normal subgroup of G, and will henceforth *not distinguish* them.'' In any case, I advise you not to adopt this phrase of his.)

I.3:3. (a) Let $A_0 \subseteq A$ and $B_0 \subseteq B$ be subgroups of a group G. Prove the following equalities. (The product-sets named are not assumed to be subgroups.)

$$(A B_0) \cap B = (A \cap B)\, B_0, \qquad A \cap (A_0\, B) = A_0\,(A \cap B), \qquad (A B_0) \cap (A_0\, B) = A_0\,(A \cap B)\, B_0.$$

(b) Show using the above results (without any further calculations with group elements) that in the diagram for the Butterfly Lemma on p.21 of Lang, the three groups shown immediately above the unlabeled node have the property that the *intersection* of any two of them is the *product* of the two groups shown immediately below that node. I.e., show that each of the intersections

(1) $$(u(U\cap v))\cap(U\cap V), \qquad (U\cap V)\cap((u\cap V)\,v), \qquad ((u\cap V)\,v)\cap(u(U\cap v))$$

is equal to the product

(2) $$(u\cap V)\,(U\cap v).$$

Hint: The operation ''$\cap$'' on sets is associative and commutative, so the first expression in (1) is simply the intersection of the sets $u(U\cap v)$, U, and V. An inclusion relation holds between two of these three sets, allowing one of those two to be dropped from the expression. A similar observation applies to the second expression in (1). When these redundant terms have been dropped, each of the expressions in (1) can be transformed using one of the results of part (a).

(c) Verify that the second display on p.21 of Lang is indeed, as he claims, an instance of the third display (= the second boxed equation on p.17), gotten using for ''H'' and ''N'' the groups named on the line after the latter display. Thus, you need to show that H is contained in the normalizer of N, and that the intersection and product sets in the third display equal the appropriate sets in the second display.

I.3:4. Let G be a group and S a subset of G. We claim there is a *least* normal subgroup N of G containing S, i.e., a normal subgroup which contains S, and is contained in every normal subgroup containing S.

There are two natural ways of constructing this subgroup: as an intersection, and as the closure of S under appropriate operations.

(a) Prove the existence of such an N in one of the above ways, and describe precisely the other approach (without going through the proof that it gives the desired group).

(b) Show that if S is closed in G under conjugation (i.e., if for all $s\in S$ and $g\in G$ one has $gsg^{-1}\in S$), then the above subgroup coincides with the subgroup of G generated by S. Deduce from this the normality statement of I:L3.

The group N described above can be called ''the normal subgroup of G generated by S''. (Lang avoids this wording, perhaps feeling that it would suggest that N is generated by S as a group; e.g., in the next-to-last sentence on p.68 he simply calls it the smallest normal subgroup containing S.)

(c) Suppose G is a group, H a subgroup, and S a subset of H. Let N_1 be the normal subgroup of H generated by S, and N_2 the normal subgroup of G generated by S. Prove an inclusion that must hold between N_1 and N_2, but show by example that these subgroups need not be equal, even if H is normal in G.

Note on I:L4 (p.75): This result is proved (without the assumption $K\subset N_H$) as display (c9) of this Companion. (The assumption $K\subset N_H$ has the advantage of guaranteeing that the set HK is a group; but the result is true without it.)

I.4:1. Show that if m and n are positive integers, there is a nontrivial homomorphism from the cyclic group of order m to the cyclic group of order n if and only if m and n are *not* relatively prime. (Hint: To prove concisely that a homomorphism exists from one cyclic group to another which sends the given generator to the desired image, note that Z_m can be described as the factor-group of $\mathbf{Z}$ by the subgroup $m\mathbf{Z}$, and that the *universal property of factor-groups* (triangular diagram on p.14 of Lang) shows just what is required to obtain a homomorphism on a factor-group.)

I.4:2. (a) Show that if a group G is generated by a set S of elements such that every two elements of S commute, then G is abelian.

(b) Deduce that if G is a group with center C, and G/C is cyclic, then G is abelian, i.e., G/C is trivial.

(c) Deduce I:L7 (p.75).

I.4:3. ¤(a) Show that if a group has a largest proper subgroup (i.e., a proper subgroup that contains all other proper subgroups), then it is cyclic of finite order.

(b) For which positive integers n does the cyclic group of order n have a largest proper subgroup?

(c) Show that a group having a smallest nonzero subgroup need not be cyclic. (Hint: Look at the groups described at the bottom of p.9.)

I.4:4. Let's see how far we can generalize the first two parts of the preceding exercise.

¤(a) Show that if a group G has proper subgroups H_1 and H_2, such that every proper subgroup of G is contained either in H_1 or in H_2, then G again must be cyclic of finite order.

(b) For which positive integers n does the cyclic group of order n have the property of part (a)?

Clearly, this above ''pattern'' cannot continue with the ''1'' of the preceding exercise and the ''2'' of part (a) above replaced by arbitrarily large integers, since that would imply that every finite group was cyclic! In fact, things start to change at the next step:

*(c) Show that if a group G has proper subgroups H_1, H_2 and H_3 such that every proper subgroup of G is contained in one of these, then either G is cyclic of finite order, or G has a homomorphism onto $Z_2 \times Z_2$.

(d) For which positive integers n does the cyclic group of order n have the property assumed in part (c)? Show that the groups having that property also include $Z_2 \times Z_2$ itself, and the two nonabelian groups of order 8 described at the bottom of p.9 of Lang.

(We will continue the investigation of these groups in Exercise I.6:7.)

I.5:1. Let G be a group. A G-set S is called *transitive* if it consists of a single orbit.

(a) Let S and T be transitive G-sets, and s an element of S. Show that S and T are isomorphic as G-sets if and only if there exists $t \in T$ such that $G_s = G_t$.

Note that if H is a subgroup of G, the set of left cosets G/H can be made a G-set under left translation: $gx = \{ga \mid a \in x\}$ $(g \in G,\ x \in G/H)$, and that this G-set will be transitive. Now

(b) Show using (a) that every transitive G-set S is isomorphic to G/H for some subgroup H of G.

(c) For S, T, s as in (a), generalize the result of (a) to a criterion for there to exist a *homomorphism* $S \to T$ as G-sets.

(d) Suppose we are given transitive G-sets S and T, and we know the isotropy subgroups $H = G_s$ and $K = G_t$ of some $s \in S$ and some $t \in T$. Express the criteria of (a) and (c) above in terms of H and K. (Note that we are concerned with criteria for there to be *some* isomorphism or homomorphism between the indicated G-sets; not necessarily one that takes s to t! So, to express the criterion of (a), you need to find a group-theoretic condition on H and K which is equivalent to the statement that there exists a $t' \in T$ with $G_{t'} = G_s$; and you need to adapt similarly the condition you got in (c).)

I.5:2. [>I.5:1] (a) Show that if G is a finitely generated group, then for each nonnegative integer n there are, up to isomorphism, only finitely many n-element G-sets.

(b) Deduce that a finitely generated group has only finitely many subgroups of any finite index n, hence has only countably many subgroups of finite index.

The next two parts show that two weakened versions of the above statement are false.

(c) If X is a set, and G a subgroup of the additive group of all $\mathbf{Z}$-valued functions on X, then for each $x \in X$, let $G(x) = \{ f \in G \mid f(x) \text{ is even}\}$. Show that each of these groups has finite index in G. Give an example of an *uncountable* set X and a *countable* subgroup G of the above sort, such that all the subgroups $G(x)$ are distinct. (Suggestion: G might be the additive group generated by the characteristic functions of a countable family of subsets of X which separates points, i.e., has the property that for every two distinct points $x, y \in X$ one of these sets contains one of x, y but not the other.) Thus, G is a countably generated group with uncountably many subgroups of finite index.

(d) Let G be the group of permutations of the integers generated by the translation function $t\colon n \mapsto n+1$, and the permutation that interchanges 0 and 1 but leaves all other integers fixed. For every set S of *even* integers, let $G(S)$ denote the subgroup of elements of G that fix all members of S. Show that the subgroups $G(S)$ are all distinct. Thus, the finitely generated group G has uncountably many subgroups.

Lest the example of (c) lead us to think that *all* non-finitely-generated groups have uncountably many subgroups, let us note:

(e) Let p be a prime, and let G be the set of rational numbers of the form a/p^n for $a, n \in \mathbf{Z}$. Show that G forms a subgroup of the additive group of $\mathbf{Q}$, that G is not finitely generated, but that G has only countably many subgroups.

I.5:3. (a) Let G be a group, H a subgroup, and S a transitive G-set with an element s such that $G_s = H$. Let $U \subseteq S$ be the fixed-set of H, i.e., the set of $u \in S$ such that $(\forall\, h \in H)\, hu = u$. Show that if H either has finite order or has finite index in G, then $\{g \in G \mid gs \in U\}$ is the normalizer of H in G.

(b) How can the above set of elements be characterized in the general case (when H is not assumed to have finite order or index)?

(c) Show by example that in the general case, the above set need not be the normalizer. (Suggestions: Let G be the permutation group of the integers, and H the subgroup of permutations that fix all negative integers. Or, let G be the group of maps of the real line into itself of the form $x \mapsto ax+b$ for real constants $a \neq 0$ and b, and H the set of such maps such that $a = 1$ and b is an integer.)

I.5:4. (a) = I:L15 (p.76). (Hint: Count the pairs (g, s) such that g fixes s, first as a sum over g, and then as a sum over s.)

(b) Do I:L16 (p.76) without using I:L15. (Hint: G *is* the union of the *left cosets* of H, but these are disjoint. You may ignore the reference to Chapter XIII.)

(c) Show that each of the above results can be deduced easily from the other.

(d) State the lower bounds that your proofs of (a) and (b) give for the number of elements of G having no fixed points, respectively the number of elements not in the union of all conjugates of H.

I.5:5. If G is a group and N a normal subgroup, let $\mathrm{Aut}(G, N)$ denote the group of those $\sigma \in \mathrm{Aut}(G)$ such that $\sigma(N) = N$.

(a) Show that every $\sigma \in \mathrm{Aut}(G, N)$ induces a $\sigma' \in \mathrm{Aut}(G/N)$, and that this construction yields a homomorphism $\mathrm{Aut}(G, N) \to \mathrm{Aut}(G/N)$.

(b) Show by examples that the above homomorphism need not be one-to-one or onto.

(c) We clearly also have a restriction homomorphism $\mathrm{Aut}(G, N) \to \mathrm{Aut}(N)$; combining this with the homomorphism of (a), we get a homomorphism $\mathrm{Aut}(G, N) \to \mathrm{Aut}(N) \times \mathrm{Aut}(G/N)$. Is this always one-to-one? Onto?

I.5:6. Let G be a group of permutations of a set S, and n a positive integer. One says that G is *n-transitive* (or that it acts *n-transitively* on S, or that S is an n-transitive G-set) if S has at least n elements, and if whenever $s_1, \ldots, s_n$, $t_1, \ldots, t_n$ are elements of S such that $s_1, \ldots, s_n$ are distinct and $t_1, \ldots, t_n$ are distinct, there exists a $g \in G$ such that $g(s_1) = t_1, \ldots, g(s_n) = t_n$.

(a) Show that for all n and m with $m \leq n$, the symmetric group S_n is an m-transitive group of permutations of $\{1, \ldots, n\}$.

(b) Given a positive integer n, for what values of m is the alternating group A_n m-transitive as a group of permutations of $\{1, \ldots, n\}$?

(c) Show that for p a prime, the group of permutations of the set $\mathbf{Z}/p\mathbf{Z}$ consisting of all maps $x \mapsto$

$ax+b$ $(a,\ b\in \mathbf{Z}/p\mathbf{Z},\ \ a\neq 0)$ is 2-transitive, but not 3-transitive. (This part assumes familiarity with the definition of the ring $\mathbf{Z}/p\mathbf{Z}$ of integers mod p.)

(d), (e), (f) = I:L47 (p.80), parts (a), (b), (c) respectively, excluding the last assertion of (c), which we give separately as:

(g) Show that any 2-transitive group of permutations on a set is *primitive*, in the sense defined in I:L46.

(h) Show by example that the converse to (g) is false.

I.5:7. (a) Show by example that Exercise I:L38(d) (p.79) does not remain true if we delete the condition that n be prime.

(b) Show, however, that again becomes true if we add the condition $s = r+1$.

Of course, (a) and (b) will be subsumed if you do (c), which is not as hard as it might seem.

(c) Determine necessary and sufficient conditions on n, r and s for S_n to be generated by $[123\ldots n]$ and $[rs]$.

One may ask, further

(d) Given a transitive subgroup $G\subseteq S_n$, must there be a transposition $[rs]$ which, together with G, generates S_n?

I.5:8. Let G be a group, S a transitive G-set, s an element of S, and $H = G_s$. Let $\mathrm{Aut}(S)$ denote the group of *automorphisms* of S (invertible homomorphisms $S\to S$) as a G-set. Prove that $\mathrm{Aut}(S)\cong N_H/H$.

Note on I:L57 (p.82, based on §I.5): Both the Examples at the end have the hypothesis $X = GY$ from the preceding paragraph. In Example 2, I think ''discretely'' just means that there is no assumption that the operation is continuous in G. (If so, the word is superfluous, since G was assumed discrete.)

I.6:1. [>I.4:2 and I.5:5(a)]. (a) = I:L24 (p.77). (Suggestions: Get commutativity with the help of Theorem I.6.5 and I.4:2(b) above. If the group has exponent p, show with the help of Proposition I.2.1 that it is isomorphic to $Z_p\times Z_p$, while if it does not have exponent p, show that it is isomorphic to Z_{p^2}.)

(b) Show that if a p-group H acts on a nontrivial p-group G by automorphisms, then its fixed group is nontrivial. (Hint: You hardly need to use the fact that G is a group.)

Now in the situation of (b), if the fixed subgroup is a normal subgroup N, then I.5:5 becomes applicable, and allows you to apply (b) above to G/N as well. This can help you get the remaining two parts:

(c) Suppose G is a group isomorphic to $Z_p\times Z_p$, and θ is an automorphism of G of order p. Show that G is generated by two elements a, b such that $\theta(a) = a$ and $\theta(b) = ab$. Show that this is equivalent to saying that there exists an isomorphism $\alpha: G\cong Z_p\times Z_p$ under which θ corresponds to the automorphism φ of $Z_p\times Z_p$ given by $\varphi(i,j) = (i,j+i)$. (Indicate the precise sense in which θ ''corresponds to φ under α''.)

(d) Show that if G is a group isomorphic to Z_{p^2}, the only automorphisms of G of exponent p are the powers of the map $a\mapsto a^{1+p}$.

I.6:2. [>I.6:1]. Let p be a prime. We shall determine here the structures of all noncommutative groups of order p^3.

Suppose G is such a group. By Corollary I.6.6, G has a normal subgroup of order p^2; moreover, by Lemma I.6.7 every subgroup of G of that order is normal. Let us now consider three cases:

(i) G has a normal subgroup N isomorphic to $Z_p\times Z_p$, say generated by elements b and c, and also has an element a of order p outside of N. Deduce that G is a semidirect product of N and the subgroup H generated by a. Show that by choosing generators b and c of N appropriately, one can get c to commute with a, and to satisfy $a^{-1}ba = bc$. Assuming the generators are so chosen, obtain a precise description of the multiplication of G on elements $a^i b^j c^k$.

Now by I.6:1(a), *either* (i) above holds *or* G has a normal subgroup N isomorphic to Z_{p^2}, say with cyclic generator b. (Conceivably, both may be true.) Assuming the latter condition, let a be an element of G not in N. Show that a cannot have order p^3. Thus there are two cases:

(ii) The order of a is p. Deduce that G is again a semidirect product of N and the cyclic group H generated by a, and that this time, by a change of generator of H, i.e., by replacing a if necessary by another generator, one can make $a^{-1}ba = b^{p+1}$. Again, describe the multiplication explicitly.

(iii) The order of a is p^2. Again show that by modifying the choice of a, one can make $a^{-1}ba = b^{p+1}$. Show also that by modifying the choice of b, one can get $b^p = a^p$. Now if we let H denote the subgroup of G generated by a, then the action of H on N by conjugation allows one to construct a semidirect product group of order p^4. Show that G is the quotient of this group by a certain normal subgroup of order p. Verify that every element of G can be written uniquely in the form $a^i b^j$ with $0 \leq i < p$, $0 \leq j < p^2$, and describe the multiplication of such elements.

Thus, for every p, we have constructed three nonabelian groups of order p^3, such that every group of that order has one of these three forms. Show, now, that if $p = 2$, a certain two of these are isomorphic, if $p \neq 2$, a different two are isomorphic, and that in each case, the remaining one is not isomorphic to the others.

Thus, for each p, there are, up to isomorphism, exactly two nonabelian groups of order p^3.

(From the above facts, it follows that there must be one of constructions (i)-(iii) that we could drop from our list, and then say that for every prime p, every group of order p^3 is isomorphic to exactly one of the two groups on the list. However, for p odd, the construction we would be dropping gives a simpler description of the group in question than the one that is isomorphic to it. So I think this three-constructions-with-isomorphisms description is more enlightening than the two-groups description would be.)

I.6:3. [> 1.5:3(a)]. Except where the contrary is stated (in part (d) below), let G be a p-group.

(a) Suppose H is a proper subgroup of G, and S a transitive G-set with an element s such that $G_s = H$. Show that the set U defined as in I.5:3(a) has cardinality > 1. (Hint: you've had a result about G-sets when G is a p-group.)

(b) Deduce that the normalizer of a proper subgroup H of G is strictly larger than H.

(c) Deduce that any maximal proper subgroup of G is normal.

(d) Show that in *any* group G, a subgroup which is both maximal among all proper subgroups, and normal, must have prime index.

(e) Let G again be a p-group, and let G^p be the subgroup of G generated by all pth powers of elements of G. Show that G^p is normal.

(f) Let G^c be the *commutator subgroup* of G, defined as in Lang, p.20, top paragraph. Show that $G^p G^c$ is the intersection of all maximal proper subgroups of G. (This is called the *Frattini subgroup* of G.)

(g) Show that if S is a subset of G, the following four conditions are equivalent:

(i) S generates G.

(ii) The image of S generates G/G^c.

(iii) The image of S generates G/G^p.

(iv) The image of S generates $G/G^p G^c$.

(Can you generalize the argument by which you got (g) from (f) to a result about groups which are not necessarily p-groups?)

I.6:4. [> I.5:1]. We shall determine all nonabelian groups of order 30.

(a) Prove (by a quick application of a result in the material on ''Structures of groups of order pq'') that every group of order 15 is cyclic (= I:L6).

Now suppose G is a nonabelian group of order 30.

(b) Show by counting elements that G cannot simultaneously have more than one 3-Sylow subgroup and more than one 5-Sylow subgroup.

Thus, G must have either a normal 3-Sylow subgroup or a normal 5-Sylow subgroup.

(c) Suppose G has a normal 3-Sylow (respectively, 5-Sylow) subgroup N. Show that in G/N, a 5-Sylow (respectively, 3-Sylow) subgroup will be normal, and hence that its inverse image in G, which we shall call M, will in turn be normal. Determine the structure of M.

(d) Show that in the above situation, G will be a semidirect product of M with a group of order 2.

(e) Express M as a direct product $M = M_1 \times M_2$, and show that any automorphism of M must carry M_1 into M_1 and M_2 into M_2. Determine all automorphisms of M of exponent 2. Describe all possible structures for G (as explicit semidirect products).

(f) Show that of the groups described above, one and only one is *not* a direct product of two groups of smaller orders. In the remaining cases, describe the direct product decompositions.

I.6:5. (a) If G is a finite group, show that the following conditions are equivalent: (i) G *cannot* be embedded in a direct product of groups of smaller orders. (ii) G has a smallest nontrivial normal subgroup. (Idea: Consider maps $G \to G/N \times G/N'$. Recall that ''smallest'' means ''contained in all others''.)

(b) [> I.6:4] Deduce that the one group G of I.6:4(f) that was not a direct product of groups of smaller orders can be written as a subgroup of a direct product of groups of smaller orders. Describe these groups.

***I.6:6.** Show that for every positive integer k there exists a positive integer N such that every finite group of order $\geq N$ has an abelian subgroup of order $\geq k$. (Suggestion: First do this for p-groups.)

***I.6:7.** (a) Suppose as in I.4:4(c) that G is a group having proper subgroups H_1, H_2 and H_3 such that every proper subgroup of G is contained in one of these. You analyzed in I.4:4(d) the case where G was cyclic. Now show that if G is finite but not cyclic, then it is a 2-group. (Hint: Will a 2-Sylow subgroup of G be proper?)

I do not know whether there are any *infinite* groups satisfying the above assumptions.

*(b) Show that a finite 2-group has the property of the first sentence of (a) if and only if it can be generated by two, but not by fewer, elements.

(c) Given a group G and a positive integer n, examine the relationships among the three conditions, (i) G has a family of n (not necessarily distinct) proper subgroups, such that every proper subgroup of G is contained in at least one of these. (ii) G has $\leq n$ maximal proper subgroups. (iii) G can be written as a union of $\leq n$ proper subgroups.

In particular, try to determine what implications hold among these three conditions for all n, giving counterexamples to implications that do not always hold. Examine whether any natural restrictions, such as finiteness, finite generation, or non-cyclicity, imply any of the implications that do not hold in general.

Some additional exercises that could be given in connection with §I.6 are indicated in the paragraph preceding Exercise I.9:1.

***I.7:1.** (a) Show that the group $\mathbf{Z}^{\omega}$ of all sequences $(a_0, a_1, \ldots)$ of integers, under componentwise addition, is *not* free abelian on any generating set.

(b) Can you describe the group $\mathrm{Hom}(\mathbf{Z}^{\omega}, \mathbf{Z})$?

I.7:2. (a) Show that if M is an abelian group, and we regard it as a commutative monoid and form

$K(M)$, then the canonical map $\gamma: M \to K(M)$ is an isomorphism.

(b) On the other hand, show that if M is a commutative monoid containing an element z such that $a+z = z$ for all $a \in M$, then $K(M)$ is the 1-element group. (Such an element z is called a *zero* element of a monoid, because the element 0 has this property in the monoid formed by any ring under multiplication, though the notation there is, of course, $a0 = 0$.)

I.7:3. Let A be a free abelian group, and x an element of A. Show that x is a member of a basis of A if and only if it cannot be written ny for $n>1$ and $y \in A$.

(Hint for ''if'': Suppose x is written $\Sigma_{i\in I}\, n_i e_i$ where $\{e_i \mid i \in I\}$ is a basis of A, and the n_i are integers. Consider the subgroup of $\mathbf{Z}$ generated by $\{n_i \mid i \in I\}$.)

¤**I.7:4.** Find an example of an abelian group A which is the sum, $A = B + C$, of two *free* abelian subgroups, but which is not itself free abelian.

Of course, this means, necessarily, that this sum is not a direct sum. However, can you do this in such a way that B and/or C is a direct summand in A? (The condition that B is a direct summand means that there exists a subgroup B' such that $A = B \oplus B'$; and similarly for C.) In such a way that A is torsion-free?

Note: Exercises III:L5-III:L8 can go with §I.7, assuming a little background knowledge: For III:L5 one needs the concept of a basis of n-dimensional real Euclidean space $\mathbf{R}^n$, and for III:L8, the arithmetic of the rational numbers, and the notation $\mathbf{Q}^*$ for the multiplicative group of nonzero rationals. Some corrections to III:L6, are noted after the exercises going with §III.5 below.

I.8:1. Let G be the group of all sequences $(a_0, a_1, a_2, \ldots)$ with $a_i \in Z_4$, under componentwise addition, and let H be the subgroup of G consisting of those elements such that $2a_0 = 0$. Show that each of G and H can be embedded in the other, but that G and H are not isomorphic.

I.8:2. Suppose G is a group such that every finitely generated subgroup of G is cyclic.

(a) Show that if G is torsion-free, then G can be embedded in the additive group $\mathbf{Q}$ of rational numbers.

*(b) Show that if G has torsion, then G can be embedded in the factor-group $\mathbf{Q}/\mathbf{Z}$.

***I.8:3.** Suppose p is a prime, and define $Z_{p^\infty} = (\mathbf{Q}/\mathbf{Z})(p)$, with the ''$(p)$'' notation as in Lang (p.42, paragraph before Theorem I.8.1). Show that $\mathrm{Aut}(Z_{p^\infty})$ is uncountable.

I.8:4. [> A2.2:4(a), at end of these exercises].

(a) Show that the subdirectly irreducible finitely generated abelian groups are precisely the cyclic groups of prime-power order.

(b) Show that the subdirectly irreducible finite p-groups are the p-groups whose centers are cyclic.

(c) [> I.8:2] Assuming the results of both parts of I.8:2, show that the subdirectly irreducible abelian groups that are not finite are the groups Z_{p^∞} defined in I.8:3 above.

Remark on the next five exercises. We know from results in Lang that all finitely generated torsion abelian groups are direct sums of finite cyclic groups Z_{p^n}, and we may ask whether something like this is true without the finite generation hypothesis. The next four exercises address this question. Since the groups Z_{p^∞} defined in Exercise I.8:3 above are not direct sums of proper subgroups, any positive result along these lines will either have to allow these groups as summands along with the cyclic groups, or have some hypothesis which excludes them.

Exercise I.8:5 will show that even allowing summands Z_{p^∞}, we do not get such a direct sum decomposition for arbitrary torsion abelian groups. On the other hand, in Theorem I.8.c2 in this Companion we got a generalization of the abovementioned result from Lang to the non-finitely-generated case by strengthening the hypothesis of being torsion to a condition that in the finitely generated case is equivalent to being torsion. Two other proofs of that same result are indicated in Exercises I.8:6 and I.8:7 below. Exercise I.8:8, on the other hand, will indicate a result for arbitrary torsion abelian groups, obtained by weakening the conclusion of being a direct sum of cyclic subgroups to one that is equivalent, in the finitely generated case, to that conclusion.

Exercise I.8:9 shows that yet another result true in the finitely generated case fails for non-finitely-generated groups.

***I.8:5.** Let p be a prime, and A the torsion subgroup of $\prod_{1 \leq i < \infty} Z_{p^i}$. Show that A contains no subgroup isomorphic to Z_{p^∞}, and is not a direct sum of cyclic subgroups.

I.8:6. (Alternative proof of Theorem I.8.c2, this Companion.)

In (a)-(c), let A be an abelian group of prime-power exponent p^n. We shall write A_p for $\{a \in A \mid pa = 0\}$, and for each $i \geq 0$ we shall write $p^i A$ for the subgroup $\{p^i a \mid a \in A\} \subseteq A$.

(a) Show that one can construct, successively, subsets S_n, S_{n-1}, ..., S_1 of A_p, such that for each i, S_i is a subset of $A_p \cap p^{i-1}A$ maximal for the condition that no $s \in S_i$ lies in the subgroup of A generated by $S_n \cup S_{n-1} \cup \ldots \cup S_i - \{s\}$.

In (b) and (c) below, $S_1, \ldots, S_n$ denote sets with this property.

(b) Show that A_p is the direct sum of its cyclic subgroups $\langle s \rangle$ for $s \in \bigcup S_i$.

(c) Suppose we choose, for each element s of each S_i, an element $t \in A$ such that $p^{i-1}t = s$. (Why is this possible?) Letting T_1, ..., T_n be the sets of elements so obtained, and $T = \bigcup T_i$, show that A is the direct sum of the cyclic subgroups $\langle t \rangle$ $(t \in T)$.

(d) Deduce that every abelian group of finite exponent n is a direct sum of cyclic subgroups.

***I.8:7.** (Yet another proof of Theorem I.8.c2, with most of the work left to you this time.)

Suppose p is a prime, and A an abelian group all of whose elements have exponents a power of p. Let us call a subgroup $B \subseteq A$ *pure* if $B \cap pA = pB$.

(a) Show that the least integer i such that A has a nonzero pure subgroup of exponent p^i is the same as the least integer i such that A has a maximal cyclic subgroup of exponent p^i.

(b) Show that for i as in part (a), any pure subgroup $B \subseteq A$ of exponent p^i is a direct summand. (Hint: Show that $p^i A \cap B = \{0\}$, and that $p^i A$ can be enlarged to the desired complementary summand.)

(c) Deduce that every abelian group of finite exponent r is a direct sum of cyclic subgroups.

***I.8:8.** [> I.8:7]. Let A be an abelian p-group. Show that, up to isomorphism, one can write

$$\bigoplus_{1 \leq i \leq \infty} A_i \ \subseteq\ A\ \subseteq\ \prod_{1 \leq i \leq \infty} A_i,$$

where for each i, A_i is a direct sum of copies of Z_{p^i}. In the case $i = \infty$, Z_{p^∞} is defined as in I.8:3.

(Idea: Get decompositions $A = A_1 \oplus B_1$, $B_1 = A_2 \oplus B_2$, etc., and show that such a chain of decompositions leads to the situation of the above display, where A_∞ is the intersection of the B_i.)

I.8:9. Let A be an abelian group.

We have seen that if A is finitely generated, then it is the direct sum of its torsion subgroup A_{tor}, and a free abelian subgroup B. In the non-finitely-generated case, a torsion-free abelian group need not be *free* abelian, but we can still ask whether A will be the direct sum of A_{tor} and a torsion-free subgroup B. In (b) and (c) below we shall see two examples showing that this is not so in general (with a modified argument for case (c) given in (d)). The criterion we shall use in both (b) and (c) is proved in (a). In (e)-(f) we shall examine further properties of these examples.

(a) Show that if C is any subgroup of A, then it is a direct summand in A (i.e., there is a subgroup B of A such that $A = B \oplus C$) if and only if the canonical surjection $A \to A/C$ has a right inverse which is a group homomorphism, and that in this case, we will have $B \cong A/C$.

In the two examples below, you will be able to prove that A_{tor} is not a direct summand by showing that A/A_{tor} has properties that no subgroup of A has. To state these properties, let us say that an element a of an abelian group (written additively) is ''divisible by'' an integer n if $a = nx$ for some group element x. Of the two examples, the first will be easier to state, but the second perhaps gives better insight into why a direct sum decomposition is impossible.

(b) Let A be the direct product, over all primes p, of the cyclic groups Z_p. Show that every element of A/A_{tor} is divisible by *all* positive integers n, but that no nonzero member of A has this property. Deduce that A_{tor} is not a direct summand in A.

(c) Let p be any prime, and let $\mathbf{Z}[p^{-1}]$ denote the abelian group of all rational numbers that can be written with denominator a power of p. (This is ring-theoretic notation for ''the ring generated by adjoining p^{-1} to the integers''; but here we are using it as shorthand for ''the underlying additive abelian group of that ring''.) Let us form the factor-group $\mathbf{Z}[p^{-1}]/\mathbf{Z}$, and for each positive integer n, let $(p^{-n}\mathbf{Z})/\mathbf{Z}$ denote the cyclic subgroup thereof generated by $[p^{-n}]$ (the image in this factor-group of $p^{-n} \in \mathbf{Z}[p^{-1}]$).

The group $\mathbf{Z}[p^{-1}]/\mathbf{Z}$ is what we have previously called Z_{p^∞}; we are describing it this way because we will want to use the canonical map $\mathbf{Z}[p^{-1}] \to \mathbf{Z}[p^{-1}]/\mathbf{Z}$, which we will write $a \mapsto [a]$. Indeed, let us define the subgroup

$$A \subseteq \mathbf{Z}[p^{-1}] \oplus (p^{-1}\mathbf{Z})/\mathbf{Z} \oplus (p^{-2}\mathbf{Z})/\mathbf{Z} \oplus (p^{-3}\mathbf{Z})/\mathbf{Z} \oplus \ldots$$

to consist of all elements $(a, b_1, b_2, b_3, \ldots)$ such that $[a] = b_1 + b_2 + b_3 + \ldots$. Show that $A/A_{\text{tor}} \cong \mathbf{Z}[p^{-1}]$, so that, in particular, every element of this factor-group is divisible by all powers of p, but that no element of A which maps to a noninteger element of $\mathbf{Z}[p^{-1}]$ is divisible by all powers of p. Deduce that A_{tor} is not a direct summand in A.

(d) In example (c), determine all subgroups $B \subseteq A$ maximal for the property of being disjoint from A_{tor}, and show directly that none of these satisfies $A = B \oplus A_{\text{tor}}$.

We now look at a few related properties of these examples.

(e) In example (b), show that for every prime p, the p-torsion subgroup $A(p) \subseteq A$ *is* a direct summand in A; and in fact that there is a *unique* subgroup B_p such that $A = A(p) \oplus B_p$. What is the intersection of all the subgroups B_p?

(f) In example (c), let $x_0 \in A$ be the element $([1], 0, 0, 0, \ldots)$. Show that x_0 is divisible by p^n for all n, but that there do not exist elements $x_1, x_2, \ldots$ such that $x_0 = px_1, x_1 = px_2, \ldots, x_i = px_{i+1}, \ldots$.

Remark: The divisibility arguments of (b) and (c) above gave relatively simple ways of showing that A/A_{tor} was not embeddable in A. But one can also get examples in which the one-variable equations $a = nx$ defining divisibility are replaced by systems of several linear equations in several variables. In this way one can get examples where A/A_{tor} has no nonzero elements divisible by infinitely many integers, but A_{tor} is still not embeddable in A.

The following three exercises, though I am putting them under §I.9, could be given any time after §I.2, referring to §I.9 only for the definition of *bilinear map* in the middle of p.48. The first of these exercises goes naturally with §I.9, but the next two are appropriate any time after §I.6 has been covered.

I.9:1. If A and B are abelian groups, we note that the set of group homomorphisms $A \to B$ becomes an abelian group under the operation defined by $(f+g)(a) = f(a) + g(a)$. Let us denote this group $\mathrm{Hom}(A, B)$. For three abelian groups A, B and C, the set of *bilinear maps* $A \times B \to C$ may, in the same way, be made a group $\mathrm{Bil}(A, B, C)$. (Take these two facts for granted in your write-up.)

Show that given abelian groups A, B, C there exists an isomorphism θ: $\mathrm{Bil}(A, B, C) \to \mathrm{Hom}(A, \mathrm{Hom}(B, C))$ characterized by the formula $\theta(\beta)(a)(b) = \beta(a, b)$.

I.9:2. (a) Suppose A and B are abelian groups (written additively), and $\beta: A\times A \to B$ any bilinear map. Show that the set $A\times B$ becomes a group G_β, in general nonabelian, under the operation $(x,y)(x',y') = (x+x',\ y+y'+\beta(x,x'))$.

(b) For any two elements x, y of a group G, let us write $[x,y]$ for the commutator $xyx^{-1}y^{-1}$. (The commonest symbol for $xyx^{-1}y^{-1}$ is (x,y), but since we are working with ordered pairs $(x,y)\in A\times B$, I felt that the use of that notation for commutators could lead to confusion.) Show that the groups G_β constructed in (a) all satisfy the identity $[[x,y],z] = e$.

(c) Suppose the abelian groups A and B of part (a) both have prime exponent p. Show that if p is odd, then G_β will again have exponent p, while if $p = 2$, G_β may not have exponent 2, but will have exponent 4.

(d) Deduce from (a) that if A, B, C are three abelian groups, and $\beta: A\times B \to C$ a bilinear map, then the set $A\times B\times C$ becomes a group H_β under the operation

$$(x,y,z)\ (x',y',z') \ = \ (x+x',\ y+y',\ z+z'+\beta(x',y)) \qquad (x,\ x'\in A,\ \ y,\ y'\in B,\ \ z,\ z'\in C).$$

Deduce that these groups also have the properties stated in (b) and (c).

(e) Show that the group H_β described in (d) above can be written as a semidirect product $A\ltimes(B\times C)$ and as a semidirect product $B\ltimes(A\times C)$. (If your proof is not based on an explicit description of the maps $A \to \mathrm{Aut}(B\times C)$ and $B \to \mathrm{Aut}(A\times C)$ used in these semidirect product constructions, and the bijections between the set of 3-tuples which form H_β and the sets of pairs which form these semidirect product groups, you should determine retrospectively what these maps and bijections are. Since expressing H_β as a semidirect product $B\ltimes(A\times C)$ involves changing the order of the factors A and B, and elements of those factors do not commute with each other, the above bijection can be expected to be nontrivial in this case.)

(f) On the other hand, give an example of a group of the form G_β as in (a), with A and B both nontrivial, which is not a semidirect product of proper subgroups.

I.9:3. [> I.9:2(a), and (d) excluding last sentence]. In this exercise we will prove that for large n, there are ''many'' groups of order p^n, by a method similar to that used for monoids in Exercise I.1:2, but with bilinear maps of finite products of Z_p in place of set-maps of finite sets. Hence let us begin by counting bilinear maps.

(The results you are asked to prove below are actually true without the assumption that p is prime; I have included that assumption because p-groups form a natural interesting class of groups.)

(a) Suppose a, b and c are positive integers, and p a prime. In the abelian group $(Z_p)^a$, let $x_1,\dots,x_a$ denote the elements $(1,0,\dots,0)$, ..., $(0,0,\dots,1)$; the analogous families of elements of $(Z_p)^b$ and $(Z_p)^c$ will be denoted $y_1,\dots,y_b$ and $z_1,\dots,z_c$. Show that every bilinear map $\beta: (Z_p)^a \times (Z_p)^b \to (Z_p)^c$ is determined by the ab elements $\beta(x_i,\ y_j)\in(Z_p)^c$, and conversely, that each ab-tuple of values in $(Z_p)^c$ can be realized as the images of this family of elements under a bilinear map. Thus, determine the precise number of bilinear maps $(Z_p)^a \times (Z_p)^b \to (Z_p)^c$. (We don't really need p to be prime here; I am just assuming this because we will want it later.)

Now by I.9:2(d), each such bilinear map β determines a group H_β with underlying set $(Z_p)^a \times (Z_p)^b \times (Z_p)^c$ (which we may think of as $(Z_p)^{a+b+c}$). To complete our argument, we need to show that not too many of these are isomorphic. It would be nice if we could say that any isomorphism between two such groups was induced by automorphisms of $(Z_p)^a$, $(Z_p)^b$ and $(Z_p)^c$, but this is not so. Rather, our trick will be to introduce some additional structure, which allows us to distinguish among the groups determined by any two bilinear maps, then show that taking away this structure does not cause too many groups to fall together.

Hence, if n is a positive integer, let an *n-pointed group* mean a system $(G,\ u_1,\dots,u_n)$, where G is a group, and $u_1,\dots,u_n$ are elements of G. A homomorphism of n-pointed groups $(G,\ u_1,\dots,u_n) \to$

$(H, v_1, \ldots, v_n)$ will mean a homomorphism of underlying groups that takes u_i to v_i for $i = 1, \ldots, n$. Now if $\beta: (Z_p)^a \times (Z_p)^b \to (Z_p)^c$ is a bilinear map, let H'_β denote the $a+b+c$-pointed group whose underlying group is H_β, defined as in Exercise I.9:2(d), and whose $a+b+c$ distinguished elements are $(x_i, 0, 0)$ $(1 \leq i \leq a)$, $(0, y_j, 0)$ $(1 \leq j \leq b)$, and $(0, 0, z_k)$ $(1 \leq k \leq c)$ (or, regarding the underlying set of H'_β as $(Z_p)^{a+b+c}$, the $a+b+c$ elements $(1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)$).

(b) Show that if a, b, c are positive integers, and β, γ are bilinear maps $(Z_p)^a \times (Z_p)^b \to (Z_p)^c$, then there exists a homomorphism $H'_\beta \to H'_\gamma$ as $a+b+c$-pointed groups if and only if $\beta = \gamma$, and that in this case, the only such homomorphism is the identity. (Warning: One may be tempted to call on the result at the bottom of p.10 of Lang, and argue that a homomorphism $H'_\beta \to H'_\gamma$ which agrees with the identity map of underlying sets on a generating set for H'_β must agree with the identity map on all elements. This is not valid, because that statement refers to uniqueness of *homomorphisms*, and till we prove what we are trying to prove, we cannot say that the identity map of underlying sets is a homomorphism $H'_\beta \to H'_\gamma$. So you need to do some calculating.) Deduce a lower bound on the number of nonisomorphic $a+b+c$-pointed groups of order p^{a+b+c}, as a function of p, a, b and c.

(c) Determine the number of $a+b+c$-pointed group structures on a group of order p^{a+b+c}. Comparing this result with those of (a) and (b), get a lower bound on the number of nonisomorphic groups of order p^{a+b+c}.

(d) Find reasonably small integers M and N such that the above result implies that the number of isomorphism classes of group of order p^M approaches infinity as $p \to \infty$, and that the number of isomorphism classes of group of order p^N is at least p^{1000}.

I.9:4. (a) Suppose A and B are abelian groups, and A_0, A_1 are subgroups of A and $f_0: A_0 \to B$, $f_1: A_1 \to B$ homomorphisms, such that for all $x \in A_0 \cap A_1$ one has $f_0(x) = f_1(x)$. Show that a homomorphism $f: A_0 + A_1 \to B$ may be defined by setting $f(x_0 + x_1) = f_0(x_0) + f_1(x_1)$.

In parts (b) through (e) below, m will be a fixed positive integer, dual groups will be defined with respect to a fixed cyclic group Z_m, and A and B, where they occur, will denote abelian groups of exponent m.

(b) Let A' be a subgroup of A, and let $\varphi \in A'^\wedge$. Show that there exists an element $\psi \in A^\wedge$ whose restriction to A' is φ. (Hint: If you have extended φ to a subgroup $A_0 \supseteq A$, and if a is an element not in A_0, let $A_1 = \langle a \rangle$, and set things up so that part (a) can be applied.)

(c) Show that $A \neq 0 \Rightarrow A^\wedge \neq 0$.

(d) If $f: A \to B$ is a homomorphism, show that f is surjective if and only if $f^\wedge$ is injective.

(e) If $f: A \to B$ is a homomorphism, show that f is injective if and only if $f^\wedge$ is surjective.

(Remark: If A and B are finite, then in view of Proposition I.9.c1, part (c) above is trivial, either of (d), (e) is immediate from the other, and even (a) is fairly easy. But for general A and B, these shortcuts are not available.)

(f) Show by example that the result of (a) fails if A and B are not assumed abelian. (Does it become true if one or the other of those groups is assumed abelian?)

I.9:5. Show by example that if, in Theorem I.9.4, we delete the assumption that A'/B' is finite, then the conclusion that $(A'/B') \cong (A/B)^\wedge$ can be false.

I.9:6. Let $(A_i)_{i \in I}$ be a family (in general infinite) of groups of exponent m.

(a) Show that $(\bigoplus A_i)^\wedge \cong \prod (A_i{}^\wedge)$.

(b) Show by example that the relation $(\prod A_i)^\wedge \cong \bigoplus (A_i{}^\wedge)$ does not in general hold.

(c) Show that of the two groups named in part (b), one can always be embedded in the other. (In fact, you should be able to describe a map that always gives such an embedding.)

I.11:1. Let $f: A \to B$ be a morphism in a category $\mathbf{C}$. Then f is called a *monomorphism* if for every object X of $\mathbf{C}$ and every pair of morphisms $i, j: X \to A$, we have $i \neq j \Rightarrow fi \neq fj$. Dually, f is called an *epimorphism* if for every object Y and pair of morphisms $i, j: B \to Y$, we have $i \neq j \Rightarrow \ if \neq jf$.

(a) Show that in **Set**, the monomorphisms are the one-to-one set maps and the epimorphisms are the surjective set-maps.

(b) Show that in **Monoid**, the monomorphisms are the one-to-one homomorphisms, and the class of epimorphisms includes the surjective homomorphisms.

(c) Show that the inclusion-map of the monoid of nonnegative integers under addition into the monoid of all integers under addition is an epimorphism in **Monoid**, though it is not surjective.

(d) Show that in any category $\mathbf{C}$, if $p: X \to Y$ and $q: Y \to X$ are morphisms such that $pq = \mathrm{id}_Y$, then p is an epimorphism and q a monomorphism.

I.11:2. Let $\mathbf{A}$ and $\mathbf{B}$ be categories. Show that we can define a category $\mathbf{B}^{\mathbf{A}}$ whose objects are the functors $\mathbf{A} \to \mathbf{B}$, and whose morphisms are the morphisms of functors (as defined on p.65). More precisely, show that when we define composition of morphisms and identity morphisms of functors in the obvious ways, the definition of a category is satisfied except for the axiom CAT1, and indicate briefly how to ''fix'' this deficiency.

I.11:3. [>I.11:2]. Let $\cdot\!\to\!\cdot$ denote the category having two objects, named 0 and 1, and three morphisms: id_0, id_1 and a morphism $\varphi: 0 \to 1$. (You should verify for yourself that these conditions determine an essentially unique category, but should not hand in the verification.) Thus, following the notation of the preceding exercise, $\mathbf{Group}^{\cdot\to\cdot}$ denotes the category whose objects are the functors from $\cdot\!\to\!\cdot$ to **Group**, and whose morphisms are the morphisms of functors.

(a) Describe in group-theoretic terms the data that determine an object of $\mathbf{Group}^{\cdot\to\cdot}$ (without referring to $\cdot\!\to\!\cdot$, or to the concept of functor), and what constitutes a morphism between two such objects.

(b) Show that the constructions associating to every group homomorphism $f: G \to H$ the group $\mathrm{Ker}(f) \subseteq G$ and the group $\mathrm{Im}(f) \subseteq H$ can be regarded as functors $\mathbf{Group}^{\cdot\to\cdot} \to \mathbf{Group}$.

I.11:4. Suppose $\mathbf{C}$ is a category such that any two objects X and Y of $\mathbf{C}$ have a product $X \times Y$ in $\mathbf{C}$.

(a) Show that any three objects X, Y, Z of $\mathbf{C}$ must then have a product, given by $(X \times Y) \times Z$.

(b) In this situation, show that $(X \times Y) \times Z \cong X \times (Y \times Z)$.

I.11:5. In a category $\mathbf{C}$, let us define a *retract* of an object X to mean an object Y given with morphisms $f: X \to Y$, $g: Y \to X$ such that $fg = \mathrm{id}_Y$; or, more precisely, a 3-tuple (Y, f, g) such that Y, f and g satisfy these conditions.

(a) Show that if (Y_1, f_1, g_1) and (Y_2, f_2, g_2) are retracts of the same object X, and if $g_1 f_1 = g_2 f_2$, then $Y_1 \cong Y_2$ in $\mathbf{C}$.

(b) Show, in fact, that the isomorphism constructed in part (a) will make commuting triangles with f_1 and f_2, and with g_1 and g_2.

(c) Show, conversely, that if two retracts (Y_1, f_1, g_1) and (Y_2, f_2, g_2) of an object X admit isomorphisms making such commuting triangles, then $g_1 f_1 = g_2 f_2$.

(d) Show that there exists a category $\mathbf{R}$ such that for every category $\mathbf{C}$, the set of functors $\mathbf{R} \to \mathbf{C}$ is in natural bijective correspondence with the set of families X, Y, f, g such that (Y, f, g) is a retract of X.

I.11:6. (a) Show that if G is any monoid, then one can construct a category $\mathbf{C}_G$ by taking for object-set a singleton $\{X\}$, and defining $\mathrm{Mor}(X, X) = G$, with the same composition as in the monoid G.

For the next two parts, define an ''action'' of a monoid G on an object Y of any category $\mathbf{C}$ to mean a monoid homomorphism $G \to \mathrm{Mor}(Y, Y)$.

(b) Verify that if G is a *group* and $\mathbf{C} = \mathbf{Set}$, this is equivalent to Lang's definition of an action of G on Y (§I.5).

(c) Show that if G is a monoid and $\mathbf{C}$ a category, then an object of $\mathbf{C}$ with an action of G on it is equivalent to a (covariant) functor from $\mathbf{C}_G$ (defined in (a)) to $\mathbf{C}$.

I.11:7. Let m be a positive integer, and let us write $\mathbf{FinAb}(m)$ for the category of finite abelian groups of exponent m. Show that the duality $h^{Z_m}: A \mapsto A^\wedge$ of §I.9, regarded as a contravariant functor $\mathbf{FinAb}(m) \to \mathbf{FinAb}(m)$, takes short exact sequences to short exact sequences. (Cf. Corollary I.9.2.) (Note our slight abuse of notation: strictly speaking, h^{Z_m} should denote a functor to $\mathbf{Set}$; but we are extending this symbol to mean the functor to $\mathbf{FinAb}(m)$ gotten by putting the natural abelian group structures on these hom-sets.)

I.12:1. Let $F = \langle ..., y_{-1}, y_0, y_1, ... \rangle$ be the free group on a denumerable set of generators $\{y_i \mid i \in \mathbf{Z}\}$, and let $\langle x \rangle$ be an infinite cyclic group (the free group on one generator).

(a) Show that there exists a unique homomorphism $\psi: \langle x \rangle \to \mathrm{Aut}(F)$ such that $\psi(x)(y_i) = y_{i+1}$ for each $i \in \mathbf{Z}$.

(b) Show that the semidirect product $\langle x \rangle \ltimes_\psi F$ is *free* on the two elements x, y_0.

Remark: both parts, (a) and (b) above, can be done via messy calculations, or elegantly, with the help of the universal property of free groups!

I.12:2. (a) Show that the following four groups are isomorphic. (It is up to you to discover the isomorphisms. I said in the discussion of semidirect products that the group described in (iii) is called the ''infinite dihedral group''. Actually, since the groups described below are isomorphic, that term may be defined in any of these four ways.)

(i) The group of maps $T_{a,b}: \mathbf{Z} \to \mathbf{Z}$, where $T_{a,b}(n) = an+b$, for $a \in \{\pm 1\}$, $b \in \mathbf{Z}$. (This is the set of all *distance-preserving* set-maps $\mathbf{Z} \to \mathbf{Z}$, but I don't ask you to prove that.)

(ii) The group with presentation $\langle x, y \mid x^2 = e,\ yx = xy^{-1} \rangle$.

(iii) The group $Z_2 \ltimes_\psi \mathbf{Z}$, where $\psi: Z_2 \to \mathrm{Aut}(\mathbf{Z})$ sends the nonidentity element of Z_2 to the automorphism $n \mapsto -n$ of $\mathbf{Z}$.

(iv) The coproduct of two copies of the group Z_2. (Write these two copies $\{e, u\}$ and $\{e, v\}$, for uniformity of notation.)

(b) Show that in the group (iv) above, every cyclic subgroup generated by an element of the form $(uv)^c$ is normal, and that with three exceptions, every normal subgroup of this group has this form.

I.12:3. Let F be the free group on a denumerable set $\{x_1, ..., x_n, ...\}$. Given an element $w \in F$, a group G is said to *satisfy the identity* $w = e$ if every homomorphism $F \to G$ carries w to e. A class $\mathbf{V}$ of groups is called a *variety of groups* if there exists some $S \subseteq F$ such that $\mathbf{V}$ is the class of groups satisfying the identities $w = e$ for all $w \in S$.

(a) Verify that the following classes of groups are varieties: (i) the class of all groups, (ii) the class of all abelian groups, (iii) the class of all groups of exponent 50, (iv) the class of all abelian groups of exponent 50, (v) the class of all trivial groups (i.e., up to isomorphism, ''the'' trivial group).

In *one* of cases (ii)-(iv) above, show explicitly how the definition given above of what it means for a group to satisfy an identity (via homomorphisms $F \to G$), when applied to the identities you give, is equivalent to the ordinary definition of the class of groups named. In the remaining cases, you may simply display an S which ''obviously'' works in the same way.

(b) Show that for each positive integer n, the class $\mathbf{Solv}_n$ of all groups G admitting a normal tower of height n with abelian factors:

$$G = G_0 \ \triangleright\ ...\ \triangleright\ G_n = \{e\} \qquad \text{with } G_i / G_{i+1} \text{ abelian,}$$

is a variety.

(c) Suppose X is *any* set, $F(X)$ the free group on X, and $w \in F(X)$. Let us define the condition that a group G ''satisfies the identity $w = e$'' exactly as in the case $X = \{x_1, \ldots, x_n, \ldots\}$ above. Show that for every $w \in F(X)$ there exists some $w' \in F(\{x_1, \ldots, x_n, \ldots\})$ such that a group G satisfies the identity $w = e$ if and only if it satisfies the identity $w' = e$.

(d) Let $w \in F$ (where F is again the free group on $\{x_1, \ldots, x_i, \ldots\}$). Show that the following conditions are equivalent: (i) The variety determined by the identity $w = e$ consists (up to isomorphism) of the trivial group only. (ii) There exists a group homomorphism $F \to \mathbf{Z}$ taking w to 1. (iii) If we denote by d_i the ''exponent-sum'' of x_i in w, i.e., the sum of all exponents to which x_i occurs, counting signs, in the expression for w, then the greatest common divisor of $\{d_1, \ldots, d_i, \ldots\}$ is 1.

(This shows that if you write down an identity at random, it is likely not to define an interesting variety.)

I.12:4. [> I.12:3(a)]. (a) Show that for every class $\mathbf{C}$ of groups, there exists a *least* variety $\mathbf{V}$ of groups containing $\mathbf{C}$.

The next four parts will show how to construct the groups in $\mathbf{V}$ from those in $\mathbf{C}$.

If $\mathbf{C}$ is a class of groups, let us define $\mathbf{H}(\mathbf{C})$ to mean the class of *homomorphic images* of groups in $\mathbf{C}$, $\mathbf{S}(\mathbf{C})$ to mean the class of groups embeddable in groups in $\mathbf{C}$ (i.e., groups isomorphic to *subgroups* of members of $\mathbf{C}$) and $\mathbf{P}(\mathbf{C})$ to mean the class of groups isomorphic to *products* $\prod_I G_i$ of arbitrary families $(G_i)_{i \in I}$ of groups $G_i \in \mathbf{C}$ (possibly with repeated factors).

(b) Show that every variety $\mathbf{V}$ of groups is closed under $\mathbf{H}$, $\mathbf{S}$ and $\mathbf{P}$ (i.e., that $\mathbf{V} = \mathbf{H}(\mathbf{V}) = \mathbf{S}(\mathbf{V}) = \mathbf{P}(\mathbf{V})$).

(c) Show that if $\mathbf{C}$ is any class of groups, then the class $\mathbf{HSP}(\mathbf{C})$ is closed under $\mathbf{H}$, $\mathbf{S}$ and $\mathbf{P}$.

(d) If $\mathbf{C}$ is a class of groups, R a member of $\mathbf{C}$, X a set, and $f\colon X \to R$ a map, let us say that R is ''free on X relative to $\mathbf{C}$'' if the condition defining a free group (Lang, p.66) is satisfied with ''group'' replaced by ''member of $\mathbf{C}$'' throughout. Show that if $\mathbf{C}$ is any class of groups closed under $\mathbf{S}$ and $\mathbf{P}$, then the method of proof of Proposition I.12.1 may be generalized to show that for every set X there exists a group R in $\mathbf{C}$ that is free on X relative to $\mathbf{C}$. Do not repeat that proof – just indicate what observations are used in adapting it.

(As noted in the discussion in this Companion regarding p.58 of Lang, there are various ways of talking about ''free groups'': as pairs (F, f), as universal maps f alone, or as objects F with the map f thought of as ''given''. In parts (d)-(f) of this exercise, I am following the last of these.)

(e) Let X be a set, $\mathbf{V}$ a variety of groups, $F(X)$ the free group on X, and $F_{\mathbf{V}}(X)$ the free group on X relative to $\mathbf{V}$. Show that there is a canonical surjective homomorphism $q\colon F(X) \to F_{\mathbf{V}}(X)$, and show that for any $w \in F(X)$, the identity $w = e$ holds in $\mathbf{V}$ if and only if $q(w) = e$ in $F_{\mathbf{V}}(X)$.

(f) (Birkhoff's Theorem, for the case of groups) Show with the help of the preceding results that for any class $\mathbf{C}$ of groups, $\mathbf{HSP}(\mathbf{C})$ is the least *variety of groups* containing $\mathbf{C}$. (Hint: We did not use ''$\mathbf{H}$'' in part (d).) Deduce in turn that a class of groups is a variety if and only if it is closed under $\mathbf{H}$, $\mathbf{S}$ and $\mathbf{P}$.

I.12:5. Show that the *free abelian group* on generators $x_1, \ldots, x_n$ may be presented *as a group* by the n generators $x_1, \ldots, x_n$, and the $n(n-1)/2$ relations $x_i x_j = x_j x_i$ $(1 \leq i < j \leq n)$.

***I.12:6.** [cf. I.12:5.] Show that no presentation of the free abelian group on n generators *as a group* can involve fewer than $n(n-1)/2$ relations.

(Suggestion: First try to show that if F is the free group on generators $x_1, \ldots, x_n$, then the commutator subgroup of F cannot be generated as a normal subgroup of F by fewer than $n(n-1)/2$ elements. Then try to get the above statement from this.)

I.12:7. Lang asserts in the first Example on p.69 that in the group presented by three generators x, y, z and the three relations

(1) $$[x,y] = y, \qquad [y,z] = z, \qquad [z,x] = x,$$

one has $x = y = z = e$. Clearly, this is equivalent to saying that in any group with three elements x, y, z satisfying the above relations, $x = y = z = e$ holds.

Below, we shall prove this assertion, obtaining in the process some results about groups satisfying more general systems of relations. At one point we will call on a number-theoretic fact that uses an exercise from §II.1, but as we will note at the end, the case of this fact needed for the group described above can be checked by arithmetic. The exercise after this one outlines an alternative proof of Lang's assertion, with more work left to the reader.

(a) Verify that elements x and y of an arbitrary group satisfy

(2) $$[x,y] = y$$

if and only if they satisfy

(3) $$xy = y^2x,$$

equivalently, if and only if they satisfy

(4) $$xyx^{-1} = y^2.$$

(b) Suppose k is a positive integer, and G is a group containing elements $x_1, \dots, x_k$ satisfying the cyclic family of relations

(5) $$[x_1, x_2] = x_2, \quad [x_2, x_3] = x_3, \quad \dots, \quad [x_{k-1}, x_k] = x_k, \quad [x_k, x_1] = x_1.$$

Show that if one of the x_i is of finite order, then all of them are of finite order. (Idea: If $x_i^m = e$, then conjugating x_{i+1} by x_i m times must leave it fixed; but m applications of (4) gives a different answer.)

(c) Assuming $x_1, \dots, x_k$ in (b) all have finite order, let $n > 1$ be a common exponent for these elements. By the same method used in (b), show that 2^n-1 is also a common exponent for these elements. But exercise II.1:2 shows that 2^n-1 is not divisible by n. Deduce that these elements have a common exponent smaller than n, and argue from this that they are all equal to e.

We can push this further ...

(d) Deduce that if a group contains elements satisfying (5), and a relation $x_i^a x_{i+1}^b = e$ holds with the integers a and b not both zero, then all x_j equal e. (Suggestion: Conjugate the given relation by x_i and compare the result with the original.)

... and still further ...

(e) Deduce that if a group contains elements satisfying (5), and a relation $x_i^a x_{i+1}^b x_{i+2}^c = e$ holds with a and b both positive, then all x_j equal e. (Suggestion: Consider two ways of transforming the given relation. On the one hand, apply (3), with x_{i+2} in the role of y, b times, to push the third term to the left past the second. On the other hand, apply (3), with x_{i+1} in the role of y, a times, to push the second term to the left past the first. Then use the general fact that in a group, $uv = e \Rightarrow vu = e$, to rearrange the result of the latter calculation so that the unchanged term x_i^a appears on the far left; equate this with the result of the former calculation, cancel x_i^a, and apply (d).)

We now come to the messy part: Showing that when $k = 3$, i.e., when (5) has the form (1), we automatically have a relation of the sort assumed in (e).

(f) Assuming (1), multiply the relation (3) on the left by z^4. Show with the help of (3), adjusted by cyclic permutations of x, y and z, that in the left-hand side of the resulting equation, you can convert a factor z^2x to x^4z^2, then a factor z^2y to yz, then a factor x^2y to y^4x^2. Likewise show that on the right you can convert a factor z^4y^2 to y^2z, and then a factor zx to x^2z. Equating the resulting expressions, deduce that $z^2x^2y^2 = e$, and complete the proof of Lang's assertion.

Remarks: When the argument of (b)-(e) is applied to the above relation $x^2y^2z^2 = e$, we find that the m of the case of (c) that arises is 6, and the only cases of II.1:2 that are needed are $\gcd(6, 2^6-1) = 3$, and $\gcd(3, 2^3-1) = 1$, which, of course, are verifiable without appealing to II.1:2.

For $k > 3$ the group presented by (5) can be shown to be nontrivial. By (c), this gives a nontrivial finitely presented group having no nontrivial finite homomorphic images.

I.12:8. This is an alternative proof of the assertion of Lang's proved in the preceding exercise. The part which we leave to your ingenuity is

*(a) Suppose a group G contains elements x and y satisfying $[x,y] = y$. Show that $\langle x,y\rangle$ is solvable.

For the remainder of the proof, suppose G is generated by three elements x, y, z satisfying $[x,y] = y$, $[y,z] = z$, and $[z,x] = x$.

(b) Show from these relations that $G = [G,G]$. (Group-theorists call a group satisfying this condition *perfect*.)

(c) Also show from the given relations that the subgroup $\langle x,y\rangle$ contains the elements zxz^{-1}, z^2xz^{-2}, and z^2yz^{-1}.

(d) Verify that the product

$$(z^2yz^{-1})^{-1}(z^2xz^{-2})(z^2yz^{-1})(zxz^{-1})^{-1}(z^2yz^{-1})^{-1}$$

simplifies formally (without the use of the relations assumed) to $z(y^{-1}xyx^{-1}y^{-1})z^{-2} = z(y^{-1}[x,y])z^{-2}$. Conclude with the help of one of the given relations that $z\in\langle x,y\rangle$, and deduce that $\langle x,y\rangle = G$. Thus, by the result of (a) and this result, G is both perfect and solvable. However –

(e) Show that the only group that is both perfect and solvable is the trivial group.

II.1:1. (a) State and prove an analog of Goursat's Lemma (I:L5, p.75) for *rings*.

(b) Deduce a description of all subrings of the ring $\mathbf{Z}\times\mathbf{Z}$. (State your description in a form that is as simple and concrete as possible for this specific case. Recall that by ''ring'' we mean ''ring with 1'', and by ''subring'' we mean ''subring containing the same 1''.)

II.1:2. Show that if $n > 1$, then n is not a divisor of 2^n-1. (Hint: If n is odd, let p be the smallest prime dividing n, and show that the order of the image of 2 in the multiplicative group of $\mathbf{Z}/p\mathbf{Z}$ is not a divisor of n. What does this imply about divisibility properties of 2^n-1?)

Note on II:L12 (p.116): When Lang says in part (c) ''Let μ be the **Möbius function** such that ...'', he means ''Let μ be the **Möbius function**, i.e., the function defined by the equations ...''. (I do not recommend using ''such that'' in this way in your writing!)

The function μ so defined is a member of R, i.e., a map from P to K. In its definition, ''$(-1)^r$'' should thus be understood as $\pm$ the identity element $1\in K$.

Lang asserts in part (c) that the result proved there gives the *Möbius inversion formula*. That formula is given as exercise V:L21 (p.254), which can be done right now, as an application of II:L12(c). (Lang has it in Chapter V because he wants to apply it in V:L22 to finite fields.) In doing it, you may assume that the abelian group A is the additive group of a ring. (In fact, any abelian group can be embedded in the additive group of a ring.)

Note on II:L13-19 (p.116), on Dedekind rings (defined on p.88): In the last line of the page, Lang points to VII:L7 for a continuation. There is also related material in III:L11-13.

II.2:1. Let R be a commutative ring. By a *submonoid* of R we shall understand a subset containing 1 and closed under multiplication. (Another term sometimes used is ''multiplicative subset''.) We use the word ''complement'' below in its set-theoretic sense.

(a) Show that the following five statements are *equivalent*.

(i) If I is an ideal of R, and S is maximal among submonoids of R disjoint from I, then the complement of S in R is an ideal.

(ii) If S is a submonoid of R, and I is maximal among ideals of R disjoint from S, then the complement of I in R is a submonoid.

(iii) If I and S are an ideal and a submonoid of R, maximal for the property of being disjoint, then $I \cup S = R$. (Here ''maximal'' means among ordered pairs consisting of a disjoint ideal and submonoid of R, with respect to the partial ordering on such pairs that makes $(I_1, S_1) \leq (I_2, S_2)$ if and only if $I_1 \subseteq I_2$ and $S_1 \subseteq S_2$.)

(iv) If I and S are an ideal and a submonoid of R respectively, and are disjoint, then there exists an ideal $I' \supseteq I$ whose complement is a submonoid $S' \supseteq S$.

(v) If I and S are an ideal and a submonoid of R respectively, and are disjoint, then for every $r \in R$, either the ideal generated by I and r is disjoint from S, or the submonoid generated by S and r is disjoint from I.

(b) Prove (v) above, and hence all of the statements (i)-(v).
(Statement (ii) is II:L1, incidentally.)

(c) Show that an ideal of R is *prime* if and only if its complement is a submonoid of R.

Statement (iv) above, interpreted in the light of (c), is a very useful tool for constructing prime ideals. Here is an important application:

(d) Show that if I is any ideal of R, then the intersection of all prime ideals containing I is $\{r \in R \mid (\exists\, n \geq 0)\ r^n \in I\}$. (Hint: For every r not in the above set, you want to find an appropriate prime ideal that does not contain it.)

II.2:2. [> II.2:1]. Suppose R is a commutative ring, and $X \subseteq R$ a set having nonempty intersection with every nonzero prime ideal of R. Let $\langle X \rangle$ denote the multiplicative submonoid of R generated by X. Show that for every nonzero element $r \in R$, the set $\langle X \rangle$ contains some multiple of r.

II.2:3. [> II.2:1]. We know that an integral domain can be described as a commutative ring R in which $\{0\}$ is a prime ideal, and that in this situation, $\{0\}$ is the *least* prime ideal of R. If R is a commutative ring with zero-divisors, we can ask whether it still has a least prime ideal, and if not, whether it has *minimal* prime ideals (i.e., prime ideals not containing any smaller prime ideals).

(a) Show by example that a commutative ring need not have a least prime ideal.

(b) Prove that a nonzero commutative ring always has a minimal prime ideal. (Hint: Use I.2:1 to turn the question into one about the existence of a *maximal* set of some sort, and use Zorn's Lemma to prove the necessary existence statement.)

(c) Show that a prime ideal $P \subseteq R$ is minimal (among prime ideals) if and only if for every $a \in P$ there exists $b \in R - P$ and an integer $n > 0$ such that $a^n b = 0$.

II.3:1. (a) = IV:L8 (p.214). (Though Lang puts this in Chapter IV, it only requires the concepts of §II.3. The assumption that A be entire is not needed in this part, but will be needed in part (c) below.)

(b) Denoting the automorphism of $A[X]$ that carries X to $aX + b$ by $g(a, b)$, determine the law of composition of these automorphisms, and show that they form a group, which is a semidirect product of the additive group of A and the multiplicative group of units of A.

(c) = IV:L9 (p.214), but adding after ''automorphism of $A[X]$'' the words ''inducing the identity on A''. (If you have seen §III.1, this means we are looking at automorphisms as an *A-algebra*.)

(d) Show that if A is a field, then every endomorphism of $A[X]$ *as a ring* carries A into itself, and that every *automorphism* of $A[X]$ as a ring carries A *onto* itself.

(e) Show that if A is a field, the group of all automorphisms of $A[X]$ as a ring is a semidirect product of the group of automorphisms of the field A, and the group of A-algebra automorphisms of $A[X]$, described in (a-c) above. What is the action of the former group on the latter?

II.4:1. Prove the assertion in the second paragraph of p.90 of Lang, that every field of characteristic 0 contains a subfield isomorphic to $\mathbf{Q}$. (You may use the results of §II.4, and the fact that the field of fractions of $\mathbf{Z}$ is $\mathbf{Q}$.)

II.4:2. (a) Show that a commutative ring is local if and only if its noninvertible elements form an ideal.

(b) = II:L3 (p.115).

II.4:3. [> III.2:1-2]. This exercise shows how to define the concept of not necessarily commutative local ring. Let A be a ring.

(a) Show that the following conditions are equivalent:

(i$_{\text{left}}$) A has a unique maximal left ideal.

(i$_{\text{right}}$) A has a unique maximal right ideal.

(ii) The set of noninvertible elements of A forms a 2-sided ideal.

(Suggestion: Translate (i$_{\text{left}}$) into a statement about left annihilators $\{a \in A \mid ax = 0\}$ of elements x of simple left A-modules.)

A ring satisfying the above equivalent conditions is said to be *local*. There are some more equivalent conditions, which for completeness I give below.

(b) Show that the conditions of part (a) are also equivalent to each of the following:

(iii$_{\text{left}}$) The set of non-left-invertible elements of A is closed under addition.

(iii$_{\text{right}}$) The set of non-right-invertible elements of A is closed under addition.

(iv) The set of noninvertible elements of A is closed under addition.

(Hint: Show that a ring satisfying (iv) cannot contain any idempotent elements, i.e., elements e satisfying $e^2 = e$, other than 0 and 1, but that a ring with right-invertible but not left-invertible elements does have such idempotents.)

In an earlier version of this Companion, I included another condition which I thought was equivalent to the above, but turned out not to be:

(c) Show that conditions (i)-(iv) above are *not* equivalent to:

(v) A has a unique maximal 2-sided ideal $\mathbf{m}$, and $A/\mathbf{m}$ is a division ring.

(If you haven't done all of parts (a) and (b), you can still do this part by obtaining a ring for which the truth-value of (v) is different from *at least one* of the other conditions listed.)

II.4:4. In the last paragraph of p.110, Lang gives three equations which say that the operation of ''localizing ideals'' respects the operations of adding, multiplying, and intersecting ideals. More generally, given any homomorphism of commutative rings, $f: A \to B$, let us, as Lang does there, write $J(A)$ for the set of all ideals of A, and let us define $f_*: J(A) \to J(B)$ to take each ideal $\mathbf{a} \in J(A)$ to the ideal $B\, f(\mathbf{a}) \in J(B)$, and $f^*: J(B) \to J(A)$ to take $\mathbf{a} \in J(B)$ to $f^{-1}(\mathbf{a}) \in J(A)$.

(a) Of the three equations Lang proves for the operation ''$S^{-1}(-)$'', determine which hold for the operation f_* for every homomorphism f of commutative rings. Prove the equations that hold, and give counterexamples for those that don't.

(b) Do the same for the operation f^*.

(c) Show that the operation $S^{-1}(-)$ treated by Lang is in fact f_* for f the canonical map $A \to S^{-1}A$. Assuming the results that you proved in (a) above, is the one verification given by Lang at the end of that paragraph sufficient to establish the three equations he shows?

(d) Again taking for f the canonical map $A \to S^{-1}A$, does the map f^* satisfy some or all of the same three equations?

(e) (Open-ended) What properties can you prove for the composite maps $f^* f_*$ and $f_* f^*$, either in general, or for the specific cases where f is the canonical map $A \to S^{-1}A$?

II.5:1. Let k be any field, and $k[x]$ the ring of polynomials over k in one indeterminate x. Let $k[x^2, x^3]$ denote the subring of $k[x]$ consisting of those polynomials $\Sigma\, a_i x^i$ such that $a_1 = 0$, i.e., polynomials with zero linear term. (The symbol $k[x^2, x^3]$ means that this subring is generated over k by the two elements x^2 and x^3, but I do not ask you to verify this fact.)

(a) Establish necessary and sufficient conditions on nonnegative integers $i, j \neq 1$ for x^i to divide x^j in $k[x^2, x^3]$. Show by example that this is *not* equivalent to the condition that x^i divide x^j in $k[x]$.

(b) Show that the elements x^2 and x^3 have a greatest common divisor in $k[x^2, x^3]$, but not a least common multiple. (You may take it for granted that any divisor of an element x^j is, up to multiplication by a unit, of the form x^i. Remember that ''least'' and ''greatest'' refer here to divisibility in this ring, not in $k[x]$.)

(c) Suppose a and b are any nonzero elements of any integral domain R. Show that if u and v are elements of R such that $ab = uv$, then u is a common divisor of a and b if and only if v is a common multiple of a and b. Show moreover that if u' and v' are two other elements such that $ab = u'v'$, then u is a multiple of u' if and only if v' is a multiple of v. Show, finally, that a *least common multiple* of a and b, if it exists, will be a divisor of ab, and that the same is true of a *greatest common divisor* of a and b if it exists. (In proving these statements, note that you may *not* assume that elements of the ring R have unique factorization, or even admit any factorization into irreducibles.)

(d) The results of (c) appear to imply that two nonzero elements a and b of an integral domain should have a *least* common multiple if and only if they have a *greatest* common divisor. But this contradicts the example of (b)! Find the fallacy; and verify that one direction of this ''if and only if'' *is* valid.

(e) Find two elements of $k[x^2, x^3]$ that have no greatest common divisor. (Suggestion: two common multiples of x^2 and x^3.)

II.5:2. Let R be a commutative integral domain. By a *prime element* of R we will mean a nonzero element p such that pR is a prime ideal. Show that the following conditions are equivalent:

(i) R is a unique factorization domain.

(ii) Every irreducible element of R is prime, and there is no infinite strictly increasing chain of principal ideals, $Ra_1 \subsetneq Ra_2 \subsetneq \ldots$.

(iii) Every nonzero nonunit in R is a product of prime elements.

II.5:3. [> II.2:1, II.5:2] In the context of II.5:2, show that conditions (i)-(iii) of that exercise are also equivalent to each of:

(iv) Every nonzero prime ideal of R contains a nonzero principal prime ideal.

(v) R has no infinite strictly increasing chain of principal ideals, $Ra_1 \subsetneq Ra_2 \subsetneq \ldots$, and satisfies the *factorization refinement property:* For any relation $ab = cd$ holding among nonzero elements of R, there exist elements $w, x, y, z \in R$ such that $a = wx$, $b = yz$, $c = wz$, $d = xy$.

Suggestions for proving that (iv) implies one of the other conditions: Use II.2:2 with X the set of nonzero prime elements of R, or II.2:1 with S the monoid generated by these elements. You may also want to review how Lang proves that a PID (in his language, a ''principal ring'') is a UFD (a ''factorial ring''), though he doesn't do all parts of that proof in the smoothest possible way.

***II.5:4.** Find an example of a commutative ring R with elements x and y such that $xR = yR$, but such that there does not exist a unit $u \in R$ such that $y = ux$.

II.5:5. Let A be an integral domain and K its field of fractions.

(a) Show that if A is a PID, then every subring R of K containing A is a localization $S^{-1}A$ for some multiplicative set S.

(b) Show that if A is a UFD such that every subring R of K containing A is a localization $S^{-1}A$ for some multiplicative set S, then A is a PID.

Clarification of II:L5 (p.115): Change ''with primes p'' to ''where p is a prime'', and ''units u'' to ''where u is a unit''.

II.5:6 [> II:L4, II:L10]. Let R be the ring of trigonometric polynomials, defined in the last paragraph before the exercises on p.114, and studied in II.5:10. Let $R[i]$ denote the ring of complex-valued functions on the real line of the form $u + v\,i$ with $u, v \in R$.

(a) Show that $R[i]$ is generated over $\mathbf{C}$ by the function e^{ix} and its multiplicative inverse.

(b) Show that $R[i]$ is a localization of a polynomial ring, and deduce that it is a principal ideal domain.

For the remainder of this exercise, let $I_0 \subseteq R$ denote the set of trigonometric polynomials $f \in R$ that satisfy $f(0) = 0$.

(c) Show that I_0 is a non-principal ideal of R.

Thus, R is not a principal ideal domain. However, the remaining parts will show that it has properties very close to those of a principal ideal domain.

(d) Show that for every ideal $J \subseteq R$, there exists a unique ideal $J' \subseteq R[i]$ closed under complex conjugation and satisfying $J' \cap R = J$. (Remark: This will of course remain true if we delete the ''closed under conjugation'' condition; but then uniqueness can fail. You might look for an example of this.)

(e) If we apply part (d) to the ideal I_0, the corresponding ideal of $R[i]$ must be principal. Find a generator (or better: all possible generators) of this ideal. Why do these elements fail to give generators of I_0 over R, contradicting (c)?

(f) Let J be a nonzero ideal of R, J' the ideal of $R[i]$ described in (d), and $f \in R[i]$ a generator of J'. Let n be the number of zeroes of f on the interval $[0, 2\pi)$, counting multiplicity. Show that the ideal J is principal if and only if n is even.

(g) Deduce that for every nonzero ideal $J \subseteq R$, exactly one of the ideals J and $I_0 J$ is principal.

Remark: From (g), one can deduce that R is a *Dedekind domain*, a concept briefly mentioned by Lang under the name ''Dedekind ring'' on p.88, and studied further in Exercises II:L11-19 and other exercises in later chapters. The idea that principal ideals of R are to all ideals as even integers are to all integers, suggested by (g), can be made precise by deducing from (g) that the *ideal class group* of R (also defined on p.88) is isomorphic to Z_2.

Historically, Dedekind domains arose in number theory, and the examples that specialists are most familiar with come from that subject. I think they would consider this one a somewhat exotic example.

Notes on exercises in Lang: II:L9 belongs under Chapter IV. It is essentially worked in this Companion, immediately following Theorem IV.1.c2.

Hint to II:L10(c): If $a + b\sqrt{(-D)}$ is a unit of R, consider the product of this element with its complex conjugate.

III.1:1. [> §II.4]. As noted in the remarks on this section, we will call a morphism $f: A \to B$ in a category an ''epimorphism'' if for any object C and any morphisms $g, g': B \to C$, one has $gf = g'f \Rightarrow g = g'$, rather than using the meaning Lang gives this term.

(a) Show that in the category of left modules over a ring R, the epimorphisms are precisely the surjective homomorphisms. (Hint: If f is not surjective, take for g and g' a zero map and a nonzero map into an appropriate object.)

(b) Show, on the other hand, that if R is a commutative ring and S a multiplicative system in R, then the natural map $R \to S^{-1}R$ is an epimorphism in the category of commutative rings, but that such maps are not in general surjective.

III.1:2. In a ring R, the *centralizer* of a subset X is defined (as in a group or semigroup) to be $\{r\in R \mid (\forall\, x\in X),\ rx = xr\}$.

(a) Show that the centralizer of any subset of a ring is a subring.

(b) Suppose R is a ring, M an R-module, $\mathrm{End}_{\mathbf{Z}}(M)$ the ring of *abelian group endomorphisms* of M, and $\mathrm{End}_R(M)$ the ring of *R-module endomorphisms* of M. Recall that the R-module structure of M is given by a homomorphism $\varphi\colon R \to \mathrm{End}_{\mathbf{Z}}(M)$. Show that $\mathrm{End}_R(M)$ is the centralizer of $\varphi(R)$ in $\mathrm{End}_{\mathbf{Z}}(M)$.

(If you have read as far as my comment to p.124 of Lang, to the effect that many noncommutative ring-theorists follow the convention that endomorphisms of right modules are written to the left of module elements and vice versa, note that we are *not* following this convention in this exercise – since we are here looking at ring-element actions and module-endomorphisms as members of a common ring $\mathrm{End}_{\mathbf{Z}}(M)$!)

The remaining point is an example of a recurring mathematical pattern, worth noting.

(c) Let R be a ring, and for every subset $X \subseteq R$, let us abbreviate the centralizer of X in R by X^*. Show that for every X, we have $X^{**} \supseteq X$ and $X^{***} = X^*$.

(When R is the ring of endomorphisms of an abelian group, and X is a subring thereof, so that we are in the situation of the preceding parts, then X^* is called the *commutant* of X, and X^{**} the *bicommutant*.)

III.1:3. In the *Sketch of Proof* of Lemma III.1.c1 in this Companion, the words ''It is easy to verify'' occur three times. Give these three verifications.

Note on III:L10 (p.168, based on §III.1) [> III:L9, p.167]. Suggested plan of attack: Given a multiplicative set S, determine what elements of M go to zero under the natural map $M \to S^{-1}M$. Hence, given a prime ideal $\mathbf{p}$, determine what elements go to zero under $M \to M_{\mathbf{p}}$. Then show that for every nonzero $x\in M$, there is a maximal ideal $\mathbf{p}$ which does not make x go to zero.

III.1:4. Let A be a ring. In the next-to-last paragraph of p.118, Lang notes that if A is an integral domain and M an A-module, then the set of elements $x\in M$ whose annihilator, $\mathrm{ann}_A\, x = \{a\in A \mid rx = 0\}$, is nonzero, forms a submodule M_{tor} of M. However, the arguments showing this fail if either the assumption that A is commutative or the assumption that it has no zero-divisors is deleted.

However, for general A, there may still be one or more ways of describing a submodule of each A-module consisting of all elements whose annihilators have certain properties.

So – determine necessary and sufficient conditions on a set X of left ideals of A for it to be true that for every left A-module M, the set of elements of M whose annihilators belong to X forms a submodule M_X of M.

III.2:1. A module over a ring R is called *simple* if it is nonzero, but has no nonzero proper submodules. Show that if M is a simple R-module, then $\mathrm{End}_R(M)$, the ring of endomorphisms of M as an R-module, is a division ring.

III.2:2. For any element x of a left R-module M, one defines the *annihilator* of x by

$$\mathrm{ann}_R\, x \;=\; \{r\in R \mid rx = 0\}.$$

(a) Show that in this situation, $\mathrm{ann}_R\, x$ is a left ideal of R, and construct a module isomorphism between the submodule $Rx \subseteq M$ generated by x, and the left R-module $R/\mathrm{ann}_R\, x$. (Thus, I am asking you to verify some things I asserted without proof in a comment to p.118 of Lang in this Companion.)

A left module over a ring R is called *cyclic* if it is generated by a single element. The above result says that the structure of a cyclic R-module is determined by the annihilator of any generator.

(b) Let Rx and Ry be cyclic R-modules, with $\mathrm{ann}_R\, x = I$ and $\mathrm{ann}_R\, y = J$. Clearly, a homomorphism $Rx \to Ry$ takes x to an element of the form ay, and is therefore determined by the element a. Characterize, in terms of the left ideals I and J, those elements $a \in R$ such that there exists a homomorphism $Rx \to Ry$ taking x to ay, and determine when the homomorphisms corresponding to two such elements a and b are the same. Thus, get a description of the abelian group $\mathrm{Hom}(Rx, Ry)$.

(c) Obtain from the above result a description of the endomorphism ring $\mathrm{End}_R(Rx)$ of a cyclic R-module Rx in terms of $I = \mathrm{ann}_R\, x$. In this case, you must, of course, determine its multiplication as well as its additive group structure.

(d) [cf. III.2:1] Show that the *simple* R-modules are precisely the cyclic R-modules Rx such that $\mathrm{ann}_R\, x$ is a maximal left ideal of R.

(e) In the case where R is commutative, state the forms that the results of (b) and (c) above take, and with the help of (d) above, describe the division rings that occur as in III.2:1.

III.2:3. [cf. III.2:1]. Part (a) below gives a class of examples showing that the converse to III.2:1 is not true. Parts (b) and (c) are more difficult questions that this result suggests.

(a) Show that if R is a commutative integral domain which is not a field, and K is its field of fractions, then the underlying R-module of K is not simple, but its ring of R-module endomorphisms is isomorphic to the field K.

*(b) Find a *finitely generated* module M over a ring R such that $\mathrm{End}_R(M)$ is a division ring (possibly a field), but such that M is not simple.

To state the last part of this exercise, let us generalize the construction of part (a) as follows. Suppose $f: A \to B$ is any homomorphism of rings, and let us regard B as a left A-module by defining left multiplication by $a \in A$ to take $x \in B$ to $f(a)x$. Then we see that for every $b \in B$, the map $x \mapsto xb$ gives an endomorphism of B as left A-module. For convenience, let us write left A-module endomorphisms of B on the *right* of the elements they are applied to, and compose them accordingly. Then the above map is a ring homomorphism $B \to \mathrm{End}_A(B)$. This is clearly one-to-one, but let us ask, open-endedly,

*(c) For what ring homomorphisms $f: A \to B$ is the homomorphism $B \to \mathrm{End}_A(B)$ described above an isomorphism?

III.3:1. Let R be any ring, and $0 \to L \to M \to N \to 0$ a short exact sequence of left R-modules. Show that the following five conditions are equivalent:

(i) For every left R-module A, the induced sequence $0 \to \mathrm{Hom}(A, L) \to \mathrm{Hom}(A, M) \to \mathrm{Hom}(A, N) \to 0$ is exact.

(i′) The induced map $\mathrm{Hom}(N, M) \to \mathrm{Hom}(N, N)$ carries some element of the former abelian group to the element id_N of the latter abelian group.

(ii) For every left R-module A, the induced sequence $0 \leftarrow \mathrm{Hom}(L, A) \leftarrow \mathrm{Hom}(M, A) \leftarrow \mathrm{Hom}(N, A) \leftarrow 0$ is exact.

(ii′) The induced map $\mathrm{Hom}(L, L) \leftarrow \mathrm{Hom}(M, L)$ carries some element of the latter abelian group to the element id_L of the former abelian group.

(iii) The original exact sequence of R-modules splits (i.e., satisfies the equivalent conditions of Proposition III.3.2, p.132. Cf. the discussion of splitting in the context of abelian groups in this Companion, after the notes on the proof of Lemma I.7.2.)

III.3:2. Let A be a ring.

(a) Show that if an A-module M is the direct sum of submodules $M_1, \ldots, M_n$, then its A-module structure can be extended to a structure of $(A \times \ldots \times A)$-module (direct product ring with n factors) in such a way that the element of this ring having a 1 in the ith position and zeros elsewhere acts as the projection onto the summand M_i; and conversely, that every $(A\times ...\times A)$-module arises in this way from a direct sum decomposition.

(b) Show that if I is an infinite set, and we denote by A^I the direct product of an I-tuple of copies of A, then any A-module with a decomposition as a direct sum of an I-tuple of submodules can be given an A^I-module structure in a way analogous to the above, and that the same is true of any A-module with an expression as a direct product of an I-tuple of modules, but that there are also A^I-modules that do not arise in either of these ways.

III.4:1. Let R be a nonzero ring, M a left R-module, and X a subset of M, and let RX denote the submodule of M generated by X. Show that X is contained in a *basis* of M if and only if X is linearly independent and the factor-module M/RX is free.

***III.4:2.** Let R be the ring of all continuous real-valued functions on the interval $[0,1]$, and consider the ideal $I = \{\, f\in R \mid (\exists\varepsilon>0)\ (\forall x\in[0,\varepsilon])\ \ f(x) = 0\}$. Show that as an R-module, I is projective.

Note on III:L5: In giving a proof that follows Lang's sketch, you need to explain his ''we may assume'' step; i.e., to say how, given $v_1, ..., v_m$, and assuming his inductive hypothesis, you can modify $v_1, ..., v_m$ to get a family with the property that he says may be assumed.

III.5:1. We noted in this Companion that if R is a ring, n a positive integer, and A the ring of $n\times n$ matrices over R, and we regard the set of column vectors of height n over R as a left A-module P, then A is isomorphic as a left A-module to the direct sum of n copies of P.

Now suppose that R is a field, or more generally, a division ring, let n and A be as above, and let M be any left A-module. Let us write e_{ij} for the usual matrix units in A.

(a) Show that $e_{11}M$, i.e., $\{e_{11}x \mid x\in M\}$, may be regarded as a left R-vector-space.

(b) Let X be any basis of the above vector space. Show that for each $x\in X$, the left A-module Ax is isomorphic to P, and that M is the direct sum over X of these modules.

Thus, every A-module is projective, and is a direct sum of copies of P. (A more general result of this sort is developed in Exercise XIII.3:1.)

III.5:2. (a) Show that for any positive integer n and infinite field k, the following statements are equivalent.

(i) An affirmative answer to Open Question III.5.c4 (a).

(ii) An affirmative answer to the same question with the assumption that V is n-dimensional replaced by the statement that it has dimension at least n, and ''bases'' replaced by ''linearly independent subsets''.

(iii) As in (ii), but this time with n-dimensional replaced by $\leq n$-dimensional, and ''bases'' replaced by ''spanning subsets''.

(Remark: The assumption that k is infinite is convenient here. However, using the fact that any field k can be embedded in an infinite field, one can show that if the above results are true for all infinite fields k, they are in fact true for all fields k.)

(b) Show that the above equivalent statements imply that given a set S, and n^2 n-element subsets $S_{11}, S_{12}, \ldots, S_{nn}$, one can choose an element s_{ij} from each S_{ij} in such a way that for each i the n elements s_{ij} $(j=1,\ldots,n)$ are distinct, and for each j the n elements S_{ij} $(i=1,\ldots,n)$ are distinct.

The assertion of (b) was a longstanding open question, called the Dinitz Conjecture, till it was proved by Fred Galvin (*The list chromatic index of a bipartite multigraph*, J. Combin. Theory, Ser. B, **63** (1995) 153-158). The vector-space questions are still open, to the best of my knowledge.

Correction to III:L6 (p.166): At the start of the next-to-last line, before ''a **Z**-basis'' add ''a subgroup of finite index with''. (The statement in Lang is false. The above modified statement is almost trivial to prove, once one sees the method. I don't know any version of the statement that is correct but nontrivial to prove.)

Note also that in the next-to-last line, the subscript on $\{y_S\}$, which appears as *wes* through the first Springer printing, and as $w \in s$ in the 4th Springer printing, should be $w \in S$.

III.6:1. Let A be a commutative ring, B a commutative A-algebra, and M a B-module. Recall from Lemma III.1.c3 in this Companion (notes to Lang's p.121) that the B-module M may be regarded as an A-module by letting each $a \in A$ act on elements of M via the image of a in B. Let us denote by $M^\vee$ the A-module $\mathrm{Hom}_A(M, A)$.

(a) Show that $M^\vee$ can be made a B-module by defining, for each $b \in B$ and $f \in M^\vee$, the element $bf \in M^\vee$ via the equation $(bf)(x) = f(bx)$.

(b) Suppose A is a field, and b any element of B. Show that multiplication by b is one-to-one on $M^\vee$ if and only if it is surjective on M, and that it is surjective on $M^\vee$ if and only if it is one-to-one on M.

(c) Still letting A be a field, let $B = A[X]$, the polynomial ring over A, and let $M = B$ regarded as a module over itself. We see from part (b) that $M^\vee$ will contain nonzero elements annihilated by X and by $X+1$. Find such elements.

(Remarks: If we had not assumed B commutative, we could still have gotten a result like (a), except that a *left* B-module structure on M would have yielded a *right* B-module structure on $M^\vee$. More generally, for any A-module N and left B-module M we get a right B-module structure on $\mathrm{Hom}_A(M, N)$. If, in addition, N is a left B-module, then this induces a left B-module structure on the same set, such that these two structures together make it a (B, B)-bimodule. Within that bimodule $\mathrm{Hom}_A(M, N)$, one can characterize $\mathrm{Hom}_B(M, N)$ as a ''centralizer'', $\{f \mid (\forall\, b \in B)\ bf = fb\}$.)

III.6:2. Show that if P is a finitely generated projective left module over a ring R, then the right R-module $P^\vee = \mathrm{Hom}(P, R)$ is also finitely generated and projective, and the natural map $P \to P^{\vee\vee}$ is an isomorphism.

Note on exercises for §III.7: Most of the exercises given earlier in this Companion for §I.8 can be used as exercises for this section, with ''abelian group'' everywhere replaced by ''A-module'', where A is a principal ideal domain. For those exercises that ask for counterexamples, some additional assumptions are needed (since when A is a field, the statements to which counterexamples are being asked for tend to be true). In these cases, it might be made part of the exercises to find conditions on a principal ideal domain under which such counterexamples will exist.

III.6:3. Let k be a field, let $f: U \to V$ be a linear map of K-vector-spaces, and let $f^\vee\colon\ V^\vee \to U^\vee$ be the induced homomorphism of dual spaces.

(a) Show that $f^\vee$ is one-to-one if and only if f is onto, and that $f^\vee$ is onto if and only if f is one-to-one. (This will be easy, using an appropriate result of this section.)

(b) Regarding each of the if-and-only-if assertions of part (b) as two statements, determine which of the resulting four statements remain true if ''field K'' and ''vector space'' are replaced by ''ring A'' and ''A-module''.

(Insofar as you find counterexamples, you might see whether you can get them to satisfy to various additional conditions, such as using modules that are finitely generated, and/or free, and/or with base-ring A the integers.)

III.7:1. Let F be a free module of finite rank over a principal ideal domain R, and $D \subseteq E \subseteq F$ submodules. Must there exist a basis $\mathcal{B}$ of F such that both D and E are spanned by multiples of members of F? (Cf. Theorem III.7.8.) Give a proof or a counterexample.

III.7:2. Theorem III.7.9 in our text (as corrected in the first Springer printing) has the hypothesis that the elementary matrices in R generate $GL_n(R)$. This leads to the question: For which R is this true?

Show that this condition holds for $R = \mathbf{Z}$.

Suggestion on how to start: Given an element of $GL_n(R)$, show that by row operations one can reduce the sum of the absolute values of the entries in the first column to 1, and finally bring that column to a form with 1 in the first position and zeroes below. Show that the submatrix below and to the right of that ''1'' is then invertible.

We will generalize this result in Exercise IV.1:3.

Note on III:L14 (p.169, based on §III.9): Lang's ''Hint'' should be considered to apply to the exercise as a whole, not to part (c) in particular. In fact, it appears to me that part (c) is most easily done by using parts (a) and (b) to get one case, and a non-snake argument in the remaining two easier cases.

Note on III:L16 (p.169, based on §III.10): I would mark this ''¤''; i.e., it is essentially trivial once one makes an easy observation (at least as it is stated in all printings through the 4th Springer printing: ''Prove that the inverse limit of a system of simple groups in which the homomorphisms are surjective is either the trivial group, or a simple group''). Perhaps what Lang intends is, rather, the following. Note that here, no surjectivity assumption is made.

III.10:1. Prove that the *direct* limit of a system of simple groups is either the trivial group, or a simple group.

On the other hand, if we consider inverse limits, but delete the surjectivity assumption, we can pose

***III.10:2.** Show by example that an inverse limit of simple groups need *not* be simple.

IV.1:1. = the handout *A principal ideal domain that is not Euclidean*. (When I assign this, I generally use parts (1)-(7) as two thirds of a weekly homework assignment.)

***IV.1:2.** Suppose A is a commutative ring, and $f \in A[X]$ is a zero-divisor. Show that there exists an element $a \in A - \{0\}$ such that $af = 0$.

IV.1:3. Do Exercise III.7:2 for the more general case where R is a Euclidean domain (defined in these notes, re p.175).

IV.3:1. Part (a) below generalizes the Eisenstein Irreducibility Criterion (Theorem IV.3.1, p.183). As in the statement of that result, let A be a unique factorization domain, K its field of fractions, p a prime element of A, and $f(X) = a_n X^n + \dots + a_0 \in A[X]$.

(a) Suppose $1 \le j < m \le n$ are such that $a_i \equiv 0 \pmod p$ for all $i < m$, not all coefficients of f are divisible by p, and $a_0 \not\equiv 0 \pmod{p^{j+1}}$. Show that when f is factored into irreducibles in $K[X]$, there will be a family of at most j of these factors whose product has degree at least m. (Hint: Look at those factors of f whose constant term is divisible by p. Compare the factorization of f in $A[X]$ and its image in $(A/(p))[X]$.)

(b) Obtain Eisenstein's Criterion as a special case.

(c) Deduce, as another case, that if in the statement of Eisenstein's Criterion, the condition $a_i \equiv 0 \pmod p$ is only assumed for $i < n-1$, then f is either irreducible, or the product of a linear factor and an irreducible factor of degree $n-1$.

IV.4:1. If R is a ring, I an ideal of R, and S a subring of R, it is not hard to verify that the set $S + I = \{s + i \mid s \in S,\ i \in I\}$ forms a subring of R. I will not ask you to prove this straightforward fact; but let us see how this construction can be used to get examples of non-Noetherian rings.

(a) Show that the subring $\mathbf{Z} + x\mathbf{Q}[x]$ of $\mathbf{Q}[x]$ (consisting of all polynomials with rational coefficients, and constant term an integer) is not Noetherian.

(b) Let k be a field. Show that the subring $k + xk[x, y]$ of $k[x, y]$ (consisting of all elements in which the coefficient of each monomial y^i $(i > 0)$ is zero) is not Noetherian.

*(c) Show that the ring constructed in (a) above has the property that every *finitely generated* ideal is principal, but is not a UFD.

*(d) Show that if k is a field and n a positive integer, then $k + x^n k[x]$ is Noetherian, and in fact has the property that every ideal can be generated by $\leq n$ elements, but contains an ideal which cannot be generated by $< n$ elements.

IV.6:1. = the handout on *Solutions in radicals*. (Although this exercise seems naturally to go with §VI.7, it can be assigned any time after §IV.6, provided the terms ‘‘primitive cube roots and fourth roots of unity’’ are explained and their elementary arithmetic properties noted. I like to assign it early, and then discuss it again after we read §VI.7. As most of a week's assignment, I typically assign parts (1)-(4) and a choice of (5) or (6). Part (8) depends on material that is in Hungerford but not Lang, and so should not be assigned unless this is covered separately. Concerning part (2), the instructor should specify what results about generating sets for S_n, e.g., I:L38(a-c) and/or I.5:7, may be assumed.)

Note on IV:L12(c): The notation D_f for the discriminant is as defined on p.193; on p.204 the same element is written $D(f)$.

V.1:1. = the handout on *Lüroth's Theorem*. (As a week's assignment, I typically give parts (1)-(9). Part (13) is immediate from II.5:1 above, and so should be omitted if that exercise has been assigned.)

In the phrase ‘‘simple transcendental extension’’, defined on that handout, the word ‘‘simple’’ has its original sense ‘‘one-fold’’, in this case ‘‘generated by a single element’’. One does not call this a ‘‘cyclic extension’’ because in Chapter VI, that term will be used to mean an extension having cyclic Galois group.

¤**V.1:2.** Suppose E and F are subfields of a field K, such that every element of E is algebraic over F, and every element of F is algebraic over E. Must E and F be algebraic over $E \cap F$?

Notes on a couple of Lang's exercises in Chapter V. One direction of V:L17 (p.254, based on §V.6) is a result in the text, so the exercise is essentially to prove the converse. Exercise V:L21 is an immediate consequence of II:L12; see note on that exercise at end exercises for II.1. Hint to V:L28 (p.256, based on §V.2): Reduce to the case where the extension of odd degree has the form $k(\alpha)$, express this as $k[X]/(f(X))$, and thus translate the hypothesis into a statement about polynomials. Expect to use induction on the degree of f.

Note: Exercises VI.14:1 and VI.14:2 can actually be given at any point after §VI.1; cf. comment preceding those exercises.

VI.1:1. Let K be a finite Galois extension of a field k, with Galois group G. Since G is a group of permutations of K, we may regard k as a G-set. Let $\alpha, \beta \in K$.

(a) Show that the orbits $G\alpha = \{\lambda\alpha \mid \lambda \in G\}$ and $G\beta = \{\lambda\beta \mid \lambda \in G\}$ are isomorphic as G-sets by an isomorphism that carries α to β if and only if $k(\alpha) = k(\beta)$.

(b) Show that $G\alpha$ and $G\beta$ are isomorphic as G-sets by some isomorphism if and only if $k(\alpha) \cong k(\beta)$ as extensions of k.

(c) In the situations of (a) and (b), what interpretation does the cardinality $|G\alpha|$ have in terms of the extension $k(\alpha)$ of k?

(d) Find characterizations analogous to (a) and (b) of the situation where $G\beta$ is the image of $G\alpha$ under a homomorphism of G-sets, with and without the condition that the homomorphism carry α to β.

(e) Why have I not also asked the analog of question (d) with ‘‘homomorphic image’’ replaced by ‘‘sub-G-set’’?

The only part of §VI.2 that the next exercise assumes is Example 1 on p.269, so it can be given after covering §VI.1, with a reference to that example. I typically give this exercise as a full week's homework assignment.

VI.2:1. = VI:L8 (p.322). However, in parts (a) and (b), assume that you are working over an arbitrary field k of characteristic $\neq 2$, rather than $\mathbf{Q}$. Also begin by justifying (briefly) the statement that the roots of f may be written $\pm\alpha$, $\pm\beta$.

If you have a printing before the 4th Springer printing, there are errata to part (b) for which you should see the pages of errata. (There are three errata-listings there. Which one applies depends on the printing you have.)

In part (c), each subextension other than the base field k itself will be quadratic over an extension just below it in the lattice, and hence can be obtained by adjoining to that extension the square root of an element thereof (p.269, Example 1). Hence, try to express each subextension as obtained from k via successive adjunctions of square roots.

In doing this exercise, you may take for granted that the group that Lang calls D_8 is a 2-Sylow subgroup of S_4, and can be pictured as the group of symmetries of the square by identifying the four elements on which S_4 acts with the vertices of the square. In (b), expect to use repeatedly the observation that an element lies in k if and only if it is fixed by all members of the Galois group. All the assertions in that part, including the parenthetical one, are to be proved, even though only one assertion is preceded by ''Show that''. In (c) you may take for granted that the subgroups of D_8 are as shown in the chart on p.271, for appropriate choices of generators σ and τ satisfying the relation displayed a few lines above the diagram. In the last part of (c), where you are asked for the field associated with each subgroup of the Galois group, you may find it useful to apply the result of (b) not only over $\mathbf{Q}$, but also over some of the fields you are trying to determine.

In displaying the diagram of subextensions, you will have to choose between the arrangement that parallels the diagram of subgroups (with *smaller* subextensions, corresponding to larger subgroups, at the top) and the arrangement natural for these subextensions, with *larger* subextensions at the top. To give the grader a uniform task, use the latter arrangement. For the same reason, take τ to be complex conjugation.

The word ''lattice'' in the last sentence of (c) means ''partially ordered set in which every pair of elements has a least upper bound and a greatest lower bound''; but you are not asked to prove anything about such upper and lower bounds.

VI.2:2. (converse to VI.2:1(a), and related results). Let k be a field not of characteristic 2.

(a) Suppose K is a Galois extension of k whose Galois group G is isomorphic to the group Lang writes D_8. Show that K is the splitting field over k of an irreducible polynomial $f(X)$ of the form $X^4 + aX^2 + b$. (Hint: Find a non-normal subgroup $H < D_8$ of order 2, let N be the normal subgroup it generates, and note that K^H is generated by the square root of an element $\gamma\in K^N$.)

(b) Show that the above conclusion is also true of any Galois extension K of k having degree 4. (Suggestion: Consider separately the cases of Galois group Z_4, and $Z_2\times Z_2$.)

(c) Show that if an irreducible polynomial f of degree 4 has splitting field of degree not divisible by 3, then its Galois group is D_8, Z_4, or $Z_2\times Z_2$. Must such an f have the form $X^4 + aX^2 + b$?

(d) Show that if f is an irreducible polynomial over any field whose Galois group is the 8-element ''quaternion group'' described by Lang on p.9, then f must have degree 8.

(The study of polynomials having this Galois group is more difficult than the case of D_8, and will not be pursued further here.)

Still another variant of the theme of this and the preceding exercise is given in VI.2:6.

VI.2:3. [cf. I.5:6]. Let f be a separable irreducible polynomial of degree $n > 1$ over a field k, let K be the splitting field of f, and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in K. Show that the following conditions are equivalent:

(i) $f(X)/(X-\alpha_1)$ is irreducible in $k(\alpha_1)[X]$.

(ii) $G(K/k)$ is 2-transitive on $\{\alpha_1, \ldots, \alpha_n\}$ (as defined in Exercise I.5:6).

VI.2:4. Let k be a field, f a separable irreducible quadratic polynomial over k, and g a separable irreducible cubic polynomial over k. Let us regard the Galois group G of fg as a group of permutations of the five roots of this polynomial. Since it permutes the set of roots of f and g separately, it lies in the obvious copy of $S_2 \times S_3$ within S_5.

(a) Show that G need not contain a product of a 2-cycle in S_2 and a 3-cycle in S_3. (Hint: Find a subgroup of $S_2 \times S_3$ with appropriate properties, then note why one can realize this as a Galois group of the indicated sort.)

(b) Show, on the other hand, that if k is a finite field, then G must indeed contain the product of a 2-cycle and a 3-cycle. (This justifies an argument Lang gives on p.274, below the middle display.)

(c) Abstracting some ideas used above, deduce the following result: If a, b are elements of a finite field k, then the polynomial $(X^3 + aX + b)(X^2 + (4a^2 + 27b^3))$ has a root in k.

***VI.2:5.** Show that the primeness assumption is needed in VI:L9 (p.322) by showing that for every composite positive integer n, the analogous statement about extensions of degree n is false.

VI.2:6. Suppose K is separable quartic extension of k (an extension of degree 4).

(a) Show that if K is *not* a quadratic extension of a quadratic extension of k, then the normal closure L of K over k has an element of degree 3.

(Suggestion: Translate the field-theoretic assumptions into conditions on $G = G(L/k)$ and on the subgroup thereof corresponding to K. Then translate these in turn into conditions on G-sets, using the result that subgroups $H \leq G$ induce transitive G-sets G/H. This will turn the question into one about subgroups of a finite symmetric group, which is not hard to prove.)

(b) Show that if $\mathrm{char}(k) \neq 2$, then the condition of (a) that K is not a quadratic extension of a quadratic extension of k is equivalent to saying that K is *not* generated over k by a root of a polynomial of the form $X^4 + aX^2 + b$ as in VI.2:1-2.

(c) Show that there exist fields K and k as in part (a).

Note on VI:L10: The words ''with $n > 2$'' at the end of the second line belong in the first line, after ''degree n''. The condition ''is the symmetric group S_n'' is ambiguous: it could mean ''acts as the full group of permutations on (the subscripts of) the n zeroes of f'', or simply ''is isomorphic, as a group, to S_n''. So for completeness, show that in the situation in question, those two conditions are equivalent, before showing that they imply the results of (a) and (b).

Note on VI:L14: I believe one is expected to assume the italicized result stated in Example 7, p.274.

Notes on VI:L16: Given a Galois extension K/k, a ''normal basis'' for K/k means a set of the form $\{\sigma\alpha\}_{\sigma\in G}$ for some $\alpha \in K$, which forms a vector-space basis of K over k. So the hypothesis that $\{\sigma\,\alpha\}_{\sigma\in G}$ is a normal basis is just equivalent to saying it is a basis. In §VI.13, Lang proves that every Galois extension has a normal basis. Though we shall not read that section, this exercise, about a property that holds assuming such a basis given, is not hard to do. Note that since α is given, when Lang says ''Show that there exists a basis ... consisting of elements of the form $S(\alpha)$'' he means ''Show that there exist subsets $S_1, \ldots, S_r$ of G such that $\{S_1(\alpha), \ldots, S_r(\alpha)\}$ forms a basis ...''.

VI.3:1. = the handout on *Quadratic Reciprocity*. Part (1)(i) is immediate from a result in Lang; you may simply cite that result. (As a week's homework, I typically assign the main parts, (1)-(8), an application such as (9), and perhaps one of (11)-(13). Part (11) requires §VI.6. (10) is important, but, together with (1)-(9), would add up to too much for a week's assignment.)

VI.5:1. Below, you will work through an easy proof of XIII:L32, a beautiful result that has been rediscovered many times. The method sketched here is adapted from H. W. Lenstra, *Inventiones math.* **25**, p.299-325, Proposition 1.3.

Let K, k and V be as in XIII:L32.

(a) Define a function $\mathrm{Tr}_G\colon V \to V$ analogous to the trace function of §VI.5, and show that this function is k-linear, and takes values in the fixed k-subspace of the action of G on V.

(b) Show that if $\varphi\colon\ V \to K$ is a K-linear map, and $w \in V$ has the property that $\mathrm{Tr}(Kw) \subseteq \mathrm{Ker}(\varphi)$, then $w \in \mathrm{Ker}(\varphi)$. (Hint: Write out the relations involved, and use linear independence of characters.)

(c) Deduce that $\mathrm{Tr}(V)$ lies in no proper K-subspace of V, and conclude that it contains a K-basis of V, and that this establishes the result of XIII:L32.

VI.6:1. The relation between the additive and multiplicative forms of Hilbert's Theorem 90 suggests that addition of 1 in a field of characteristic p is analogous to multiplication by a primitive pth root of unity in a field of characteristic $\neq p$. Now recall that the *discriminant* is a polynomial in n indeterminates which gets multiplied by -1 (a primitive square root of unity) on applying any odd permutation to the indeterminates. This leads to

(a) Let n be a positive integer. Deduce from results proved in Lang that there exists a rational function r_n in n indeterminates over $\mathbf{Z}/2\mathbf{Z}$ with the property that the action of any odd permutation of the indeterminates sends r_n to r_n+1. (Recall that ''rational function'' means ''element of the field $(\mathbf{Z}/2\mathbf{Z})(t_1, \dots, t_n)$'', though the elements of such a field cannot, strictly speaking, be regarded as functions.) Show, moreover, that $r_n(r_n+1)$ is a rational function of the elementary symmetric polynomials in $t_1, \dots, t_n$.

(b) Find an explicit description of such a rational function r_n for general n.

(c) For $n = 2, 3$ obtain formulas expressing $r_n(r_n+1)$ in terms of the symmetric polynomials in the given indeterminates.

VI.6:2. Let k be a field, and E the rational function field over k in $2n$ indeterminates, $x_1, \dots, x_n$, $y_1, \dots, y_n$. Let S_n act on E by simultaneously permuting the two sets of indeterminates, so that $\sigma(x_i) = x_{\sigma(i)}$, $\sigma(y_i) = y_{\sigma(i)}$, and let K be the fixed field of this action.

(a) Show that for all i, $K(x_i) = K(y_i)$. Deduce that $K(x_1, \dots, x_n) = K(y_1, \dots, y_n) = E$.

*(b) Can you find explicit expressions for the y_i in terms of the x_i and elements of K? (I don't know whether there is an easy solution.)

Note on VI:L6: In the second sentence of part (b), for ''Let z be an element'' read ''Assume there exists an element z''. I.e., the existence of such an element is not a consequence of the preceding conditions. (If it were, the exercise would imply that every quadratic extension field was contained in a quartic extension field, which we know is not so from the case of $\mathbf{C}/\mathbf{R}$.) On the other hand, in the third line, ''Let $\alpha^2 = \gamma$'' means ''Extend E by adjoining an element α satisfying $\alpha^2 = \gamma$''.

Note on VI:L29: I suggest doing part (c) before part (b).

Note on VI:L44: Where Lang has $\lim\limits_{n\to\infty}$, the form $\varprojlim_{n\to\infty}$ might be clearer.

Note on the next two exercises below: Neither of these actually assumes material in Lang's §VI.14 or in my comments on that section; they could be given after §VI.1. I put them here because they seemed most closely related to the ideas of §VI.14.

VI.14:1. Do VI:L26 (p.325), but give the result in as much generality as your proof naturally leads to. Also see whether you can obtain from your proof any stronger condition on the Galois groups of finite subextensions of E than that they be cyclic.

***VI.14:2.** (generalization of VI:L25, p.325). Suppose K is an infinite Galois extension of a field k, and n a positive integer such that for every finite Galois subextension $E \subseteq K$, the group $\mathrm{Gal}(E/k)$ can be generated by $\leq n$ elements. Show that k is the fixed field of some n-generator subgroup of $\mathrm{Gal}(K/k)$.

VIII.1:1. Let k be a field, K an extension field, and E, F intermediate fields. Recall that EF denotes the compositum of E and F in K.

(a) Show that $\mathrm{tr.deg.}(EF/k) + \mathrm{tr.deg.}(E \cap F/k) \leq \mathrm{tr.deg.}(E/k) + \mathrm{tr.deg.}(F/k)$.

*(b) Can the inequality of (a) be strict?

Note on VIII:L1 (p.374, based on §VIII.1): The last sentence (at least as it appears in all printings through the 4th Springer printing), ''Describe all automorphisms and their cardinality,'' is unreasonable, unless one allows a very vague sense of ''Describe''. ''Determine the cardinality of the group of all automorphisms'' would be reasonable.

Note on VIII:L6: I think that $k(x)$ and $k(y')$ in the last line should be $k_u(x)$ and $k_u(y')$.

X.4:1. Let A be a ring and $\mathbf{a} \subseteq A$ a 2-sided ideal.

(a) Show that if E is a finitely generated projective left A-module, then $E/\mathbf{a}E$ is a finitely generated projective left $A/\mathbf{a}$-module.

In the remaining parts, let us suppose $\mathbf{a}$ is contained in all maximal left ideals, and in (b)-(d), let E, F be finitely generated projective left A-modules.

(b) Show that a module homomorphism $f: E \to F$ is an isomorphism if and only if the induced homomorphism of $A/\mathbf{a}$-modules, $f': E/\mathbf{a}E \to F/\mathbf{a}F$ is an isomorphism.

(c) Deduce that $E \cong F$ if and only if $E/\mathbf{a}E \cong F/\mathbf{a}F$.

(d) Show that E is isomorphic to a direct summand in F if and only if $E/\mathbf{a}E$ is isomorphic to a direct summand in $F/\mathbf{a}F$.

*(e) Show by example that $A/\mathbf{a}$ may have a finitely generated projective module P such that there is no finitely generated projective A-module E with $E/\mathbf{a}E \cong P$.

XIII.1:1. We observed in the comments on §XIII.1 that ${}^mR^n$ is a left module over ${}^mR^m$ and a right module over ${}^nR^n$, and that each of these rings acts on ${}^mR^n$ by endomorphisms as a module over the other.

Show that the endomorphisms of ${}^mR^n$ as a right ${}^nR^n$-module (when written to the left of their arguments and composed accordingly) form precisely the ring ${}^mR^m$, and likewise that the endomorphisms of ${}^mR^n$ as a left ${}^mR^m$-module (written to the *right* of their arguments and composed accordingly) form precisely ${}^nR^n$.

Suppose that ''by force of habit'' we write endomorphisms of the left ${}^mR^m$-module ${}^mR^n$ to the left of their arguments, and compose them accordingly. Describe the structure of the endomorphism ring in this case.

***XIII.2:1.** Let R be a field and n a positive integer. Show that any automorphism α of the ring ${}^nR^n$ preserves ranks of matrices; i.e., that if $A \in {}^nR^n$, then $\mathrm{rank}(\alpha(A)) = \mathrm{rank}(A)$. (Hint: Find some characterization of the rank of A purely in terms of the ring structure of ${}^nR^n$; e.g., in terms of the left or right ideal generated by A.)

***XIII.2:2.** Let the *inner rank* of a matrix $A \in {}^mR^n$ over a ring R be defined as in the notes to §XIII.2 in this Companion. Show by example that the inner rank of a matrix A over a commutative integral domain can be different from the rank of A over the field of fractions of R.

XIII.3:1. [cf. III.4:3 and XIII.1:1]. Let R be any ring, n any positive integer, and L any left ${}^nR^n$-module. Let $M = \{e_{11}x \mid x \in L\}$. Essentially as in Exercise III.4:3, this set may be regarded as a left

R-module. (I won't ask you to verify this this time.)

(a) Show that ${}^nM \cong L$ as left ${}^nR^n$-module. (Here we understand ${}^nM$ to be made an ${}^nR^n$-module, using the R-module structure on M, as in this section of Lang.)

This shows that every left ${}^nR^n$-module is, up to isomorphism, of the form ${}^nM$ for some left R-module M. Hence to ''understand'' ${}^nR^n$-modules, it remains only to describe their homomorphisms.

(b) Given left R-modules M and N, show that $\mathrm{Hom}_{{}^nR^n}({}^nM, {}^nN) \cong \mathrm{Hom}_R(M, N)$ as abelian groups.

(It follows that the category of left ${}^nR^n$-modules is equivalent to the category of left R-modules. Note, however, that under this equivalence, the free left ${}^nR^n$-module of rank r corresponds to the free left R-modules of rank nr. In general two rings having equivalent module-categories are called *Morita equivalent*. There is a general theory describing how this happens; the above is the simplest nontrivial case.)

***XIII.4:1.** This problem concerns a possible converse to XIII:L26 (p.548).

Suppose n is a positive integer, and

$$f \in \mathbf{Z}[t_{11}, t_{12}, \ldots, t_{nn}]$$

a polynomial in n^2 indeterminates, and suppose f has the property that for every commutative ring A, every n-generator ideal $I = Ax_1 + \ldots + Ax_n \subseteq A$, and every family of n^2 elements $c_{ij} \in A$, if we define $y_i = \Sigma\, c_{ij} x_j$ and $I' = Ay_1 + \ldots + Ay_n$, then we have

$$f(c_{11}, c_{12}, \ldots, c_{nn})\, I \subseteq I'.$$

Must f be divisible (as a polynomial) by $\det(t_{ij})$?

XIII.4:2. Let m and n be positive integers, and let E be a free module of rank m over a commutative ring R. Show that $L_a^n(E)$ is a free R-module, and determine its rank. (For $n = m$ you should, of course, get Corollary XIII.4.12, p.517.)

XIII.4:3. (i) = XIII:L25 (p.547). Hint: The $n = 2$ case is easy. To simplify the problem for general n, apply appropriate invertible transformations to pairs of columns.

*(ii) More generally, suppose we are given an $m \times n$ matrix A over a principal ideal domain, with $m < n$. Can you find necessary and sufficient conditions for this to be completable to an $n \times n$ matrix of determinant 1?

XIII.5:1. We have been studying the classes of symmetric and alternating bilinear forms on a free module. This exercise will examine the question of whether there are any other ''natural'' classes of bilinear forms. For simplicity, we will assume our base ring is a field.

Given a field k, let us define a ''subfunctor X of L^2'' to mean a construction associating to every finite-dimensional k-vector-space V a subspace $X(V) \subseteq L^2(V, k)$ in such a way that for every linear map $f: V \to W$ among vector spaces, the induced map $L^2(f): L^2(W) \to L^2(V)$ carries $X(W)$ into $X(V)$. Let us partially order the subfunctors of L^2 by writing $X \leq X'$ if for all V, one has $X(V) \subseteq X'(V)$.

Show that the subfunctors of L^2 are precisely L^2 itself, L_a^2, L_s^2, and 0, and determine the partial ordering on this set of four subfunctors. This ordering will depend (to a slight extent) on k.

(Remark: What we are calling $L^2(V)$ can be naturally identified with $\mathrm{Hom}_k(V \otimes_k V, k)$. A more natural form of the above question would ask for all subfunctors of the functor $V \mapsto V \otimes_k V$. The above results would follow from the answer to this question with the help of the standard correspondence between subspaces of a finite-dimensional vector space and subspaces of its dual. But I forewent this elegance to fit the question to the reading. Note also that one might generalize the original question by replacing ''bilinear'' with ''n-linear'' for fixed $n \geq 0$; equivalently, in the more natural form just mentioned, one might replace the 2-fold tensor product with the n-fold tensor product. The answer then becomes considerably more complicated!)

XIII.5:2. Let k be a field, and κ an infinite cardinal.

(a) Prove that the dual of a κ-dimensional k-vector-space has dimension at least $\max(2^\kappa, \mathrm{card}\ k)$.

Suggestion: If $\mathrm{card}\ k < 2^\kappa$, look at the cardinality of the dual space. In the contrary case, show that the dual has a subspace isomorphic to the space k^ω of all sequences of elements of k, and show that the exponential sequences $(1, c, c^2, \ldots)$ $(c \in k)$ are linearly independent.

The dual space considered in the above result is clearly isomorphic to the k-vector-space of all k-valued functions on a set of cardinality κ. It is interesting that one can get a similar result for a much more restricted space of functions:

(b) Let S be a set of cardinality κ, and V the space of k-valued functions on S that assume only finitely many distinct values. (Equivalently, the space spanned by the characteristic functions of all subsets of S.) Show that V has dimension 2^κ.

Suggestion for showing "$\geq$": Let X be a set of cardinality κ, and note why you can assume without loss of generality that S is the set of all finite subsets of X. For every subset $Y \subseteq X$, let $\varphi_Y \in V$ be the function which takes the value 1 at members of S which are subsets of Y, and 0 at all others. Show that these 2^κ members of V are k-linearly independent.

***XIV.2:1.** (Cf. Corollary XIV.2.3, p.558.) Let $A_1, \ldots, A_r, B_1, \ldots, B_r$ be $n \times n$ matrices over a field k. Assume there is an invertible matrix C' over an extension field k' of k such that $B_i = C' A_i C'^{-1}$ $(i = 1, \ldots, r)$. Must there exist an invertible matrix C over k itself with this property? If you can't answer the question in complete generality, you might see whether you can do so under some additional assumption.

XIV.3:1. (a) = XIV:L10 (p.568). (Note that while a polynomial $f(t) \in k[t]$ can be evaluated at any element of k, we can merely say that a rational function $r(t) = p(t)/q(t) \in k(t)$ can be evaluated at "almost all" elements of k, namely, those that are not roots of q, assuming our fraction written in lowest terms. Likewise, one can only say that $r(A)$ can be evaluated at "most" matrices. You should describe the sense in which one can speak of evaluating $r(A)$, and then state and prove the result asked for.)

(b) Suppose M is the matrix of an endomorphism f of a finite-dimensional vector-space V, which again satisfies the hypothesis of Theorem XIV.3.10. We know that f induces endomorphisms $L^2(f)$, $L^2_s(f)$ and $L^2_a(f)$ of the spaces $L^2(V)$, $L^2_s(V)$ and $L^2_a(V)$ respectively. Determine the characteristic polynomials of these maps.

XVI.1:1. (a) Show that if A is a nonzero finitely generated abelian group, then the tensor product $A \otimes_{\mathbf{Z}} A$ is nonzero.

In contrast:

(b) Let $p \in \mathbf{Z}$ be a prime, and let the group Z_{p^∞} be defined as in I.8:3. Show that $Z_{p^\infty} \otimes_{\mathbf{Z}} Z_{p^\infty} = \{0\}$.

*(c) Prove the analog of (a) for finitely generated modules over an arbitrary commutative ring. (Whether this part should be "starred" really depends on what previous chapters have been covered. But the next one certainly deserves its star.)

*(d) Does there exist a commutative ring k and a k-module M such that $M \otimes_k M$ is nonzero, but $M \otimes_k M \otimes_k M = \{0\}$? If you can't answer this for general k, can you answer it for $k = \mathbf{Z}$?

XVI.1:3. Let E and F be vector-spaces over a field k, and z any element of $E \otimes_k F$.

(a) Show that one can write $z = \Sigma_{i=1}^{r}\, x_i \otimes y_i$ where $x_1, \ldots, x_r$ are linearly independent elements of E, $y_1, \ldots, y_r$ are linearly independent elements of F, and $r \geq 0$.

(b) Suppose we have another expression for the same element, $z = \Sigma_{i=1}^{r'}\, x'_i \otimes y'_i$, where the x''s and y''s again form linearly independent families. Show that $r' = r$, that the space spanned by the x''s is the same as the space spanned by the x's, and that the space spanned by the y''s is the same as the space spanned by the y's. In fact, show that if we write $\mathbf{x}$ for the row vector of elements of E formed by the x's, $\mathbf{x}'$ for the row vector formed from the x''s, and likewise $\mathbf{y}$ and $\mathbf{y}'$ for the column vectors of elements of F formed from the y's and the y''s, then there exists an invertible $r\times r$ matrix U over k such that $\mathbf{x}' = \mathbf{x}U$, $\mathbf{y}' = U^{-1}\mathbf{y}$.

XVI.1:4. Let n be a positive integer and k a commutative ring, and let $\otimes^n$ denote the functor from k-modules to k-modules that takes every k-module M to the n-fold tensor product $M \otimes_k \dots \otimes_k M$, which we shall write $\otimes^n M$. Given any homomorphism $h: M \to N$ of k-modules, the induced homomorphism of n-fold tensor products will be written $\otimes^n h: \otimes^n M \to \otimes^n N$.

By an *endomorphism* f *of the functor* $\otimes^n$ we shall mean any construction associating to each k-module M an endomorphism f_M of the k-module $\otimes^n M$, which respects homomorphisms of k-modules, in the sense that for every such homomorphism $h: M \to N$, the following diagram commutes:

$$\begin{array}{ccc} \otimes^n M & \xrightarrow{\otimes^n h} & \otimes^n N \\ \big\downarrow f(M) & & \big\downarrow f(N) \\ \otimes^n M & \xrightarrow{\otimes^n h} & \otimes^n N \end{array}$$

One defines the sum of two endomorphisms of $\otimes^n$, and the result of multiplying such an endomorphism by an element of k, in the obvious ways, and one thus sees that such endomorphisms form a k-module (at least, if we ignore the question of whether they form a set!).

As an example, it is easy to see that for each element σ of the symmetric group S_n, there is an endomorphism $\bar\sigma$ of $\otimes^n$ whose action on decomposable elements is given by $\bar\sigma(x_1 \otimes \dots \otimes x_n) = x_{\sigma^{-1}(1)} \otimes \dots \otimes x_{\sigma^{-1}(n)}$. We can now state the problem:

Show that every endomorphism f of $\otimes^n$ is a k-linear combination of the endomorphisms $\bar\sigma$ $(\sigma\in S_n)$. (Suggestion: Look at the behavior of f on an appropriate ''universal'' element.)

Remark: Clearly one can also compose these endomorphisms, hence they have a natural structure of *k-algebra*. It is not hard to deduce from the above result that this algebra is isomorphic to the group algebra kS_n. But I will spare you the writing out, and myself the grading, of the verification of this fact.

XVI.1:5. [Assumes the material on *Tensor products in the noncommutative context,* this Companion.]

Let k be a field, and V a 1-dimensional k-vector-space, with basis $\{x\}$.

(i) Determine all ways to make V into a $(k[t],\ k[t])$-bimodule so that the right and left actions of elements of k agree with their actions under the given k-vector-space structure.

(ii) For every pair of bimodules E and F of the sort characterized in (i), determine the $(k[t],\ k[t])$-bimodule structure of $E \otimes_{k[t]} F$.

(iii) Show that for appropriate choice of E and F as above, one can on the one hand get $E \otimes_{k[t]} F$ nonisomorphic as a k-vector-space to $F \otimes_{k[t]} E$, and on the other hand, get these objects isomorphic as k-vector-spaces but nonisomorphic as bimodules.

XVI.2:1. Here are a few examples showing that the homomorphism of Proposition XVI.2.5 (p.610) can fail to be an isomorphism if E and F are not taken free of finite rank.

(i) Show that if R is a field, and E, F are infinite-dimensional vector spaces over R, then that homomorphism is one-to-one, but not onto.

(ii) Show that if $R = \mathbf{Z}$, $E = Z_{p^\infty}$ (see I.8:3), and $F = \mathbf{Q}$, then that homomorphism is onto but not one-to-one. (Hint: Show that $\mathrm{End}(Z_{p^\infty})$ is torsion-free as an additive group, and use this to deduce that the tensor-product of endomorphism rings is nontrivial.)

(iii) Show that if $R = \mathbf{Z}$, $E = Z_{p^2} \oplus Z_p$, and $F = Z_p$, then the homomorphism is neither one-to-one nor onto.

On the other hand, there are some nice cases not covered by the proposition in which one can show that the homomorphism is an isomorphism:

(iv) Show that if E *or* F is free of finite rank, then that homomorphism is an isomorphism. (Hint: In that case, you get a decomposition of $E \otimes F$ as a direct sum of copies of F, and can use the ideas in the comment regarding p.505, bottom, in this Companion about using matrices to represent direct homomorphisms among direct sums of modules.)

(v) Show, still more generally, that the homomorphism is an isomorphism whenever E or F is a finitely generated projective module.

XVI.3:1. (i) Suppose R is a ring and G a functor from left R-modules to abelian groups, which respects the group structure on homomorphisms; i.e., such that given $f, g: E \to E'$, we have $G(f+g) = G(f) + G(g)$. Show the equivalence of conditions **F1** and **F2** (pp.612-613) with the functor G in place of the functor $F \otimes -$ of those pages.

(ii) Show by example that these two conditions are not equivalent to **F3** in this generality, by looking at the functor $L(F, -)$ for an appropriate left R-module F. (Suggestion: Figure out to what extent such a functor *must* preserve exactness, then look for an example where the case that need *not* hold fails.)

Remark: Along with functors of the forms $F \otimes -$ and $L(F, -)$, there is one other familiar class of functors on categories of modules that respects the group structure on morphisms: the contravariant functors $L(-, E)$. Functors of each of these sorts in general preserve exactness at most, but not all parts of a short exact sequence. The F or E for which they do preserve exact sequences (in which case they are called *exact functors*) are called, respectively, *flat* modules (discussed in this section), *projective* modules (pp.137-139) and *injective modules* (§XX.4).

XVI.3:2. Prove the following partial converse to Proposition XVI.3.2: If R is a unique factorization domain, and every torsion-free R-module is flat, then R is a principal ideal domain.

(Suggestion: Reduce the problem to showing that if $x, y \in R$ have g.c.d. 1, then $xR + yR = R$, and then somehow get this equality from the fact that $xR + yR$ is flat. One way to use flatness might be to apply Lemma XVI.3.3 with $M \to F$ the natural map $xR \oplus yR \to xR + yR$, and $E = R/(xR + yR)$.)

***XVI.3:3.** This exercise will prove the implication (c)⇒(a) of Theorem XVI.3.2 by an argument close to that of Lazard's original paper.

Let E be a right R-module satisfying condition (b) of that theorem. Let H be a free right R-module on a basis $\mathfrak{B}$, given with a homomorphism $h: H \to E$ such that for every $x \in E$, infinitely many elements of $\mathfrak{B}$ are mapped to x. (For instance, we could let F be the free module on the product of the set of natural numbers and the underlying set of E, and map this to E in the obvious way.)

Now let I be the set of ordered pairs (H_i, K_i) where H_i is the free submodule of H generated by a finite subset of $\mathfrak{B}$, and K_i is a submodule of $H_i \cap \mathrm{Ker}(h)$ such that H_i / K_i is also free. For $i = (H_i, K_i) \in I$ we shall write $F_i = H_i / K_i$. Note that for each $i \in I$, the map h induces a homomorphism $h_i: F_i \to E$. Given $i = (H_i, K_i)$, $j = (H_j, K_j) \in I$, we shall write $i \leq j$ if $H_i \subseteq H_j$ and $K_i \subseteq K_j$.

(i) If $i \leq j \in I$, describe a natural homomorphism $f_{j,i}: F_i \to F_j$ over E, and show that if $i \leq j \leq k \in I$, then $f_{k,j}\, f_{j,i} = f_{k,i}$.

(ii) Show that if $i \in I$, and F is a free module of finite rank given with a homomorphism into E, and $f: F_i \to F$ is any homomorphism over E, then there exists $j \geq i$ such that F_j is isomorphic to F as a module with a homomorphism from F_i into it, and a homomorphism from it into E. (I.e., there is an isomorphism $F_j \cong F$ which makes commuting triangles with the maps out of F_i and into E.) This proof will make use of the assumption that infinitely many elements of $\mathfrak{B}$ map to each element of E, but the assumption that E satisfies (b) will not yet be needed.

(iii) Show by combining the hypothesis (b) on E and the result of (ii) that the partially ordered set I is directed, and that $\varinjlim_i F_i \cong E$.

XVI.3:4. Let R be a commutative ring and $\mathbf{m}$ a maximal ideal of R. Thus, $R/\mathbf{m}$ is a field, and $\mathbf{m}/\mathbf{m}^2$ can be regarded as a vector-space over that field.

(i) Show that if this vector-space has dimension > 1, then $\mathbf{m}$ is not flat as an R-module.

(ii) Show that all the examples of non-flat ideals given in the comment to p.614 (top two paragraphs) in this Companion are instances of this result.

XVI.3:5. (a) Suppose $0 \to N \to M \to F \to 0$ is a short exact sequence of right modules over a ring R, and $f\colon F_0 \to F$ a module homomorphism. Show how to obtain from this map a module M_0, a short exact sequence $0 \to N \to M_0 \to F_0 \to 0$, and a map of short exact sequences

$$\begin{array}{ccccccccc} 0 & \to & N & \to & M_0 & \to & F_0 & \to & 0 \\ & & \downarrow{=} & & \downarrow & & \downarrow f_0 & & \\ 0 & \to & N & \to & M & \to & F & \to & 0. \end{array}$$

(b) Verify that your construction is functorial; that is, that given maps from two free modules F_0 and F_1 into F, and a homomorphism $F_0 \to F_1$ respecting the maps into F, you get a homomorphism between your short exact sequences that respect your maps into the given sequences.

(c) Verify that your construction respects direct limits.

(d) Combining these observations with Lazard's Theorem, obtain a proof of Lemma XVI.3.3 (p.614) based on the fact that the desired result holds when F is projective (and so in particular, when it is free).

(e) Similarly, prove the first assertion of Proposition XVI.3.4 (p.615) by first establishing it when F'' is free, then applying (a)-(c).

XVI.3:6. Let $0 \to E' \to E \to E'' \to 0$ be a short exact sequence of left modules over a ring R, and F a right R-module. If F is E'-flat and E''-flat, must it be E-flat?

XVI.3:7. (Cf. XVI:L6, p.638.) Suppose E is a flat right R-module and F is an (R,S)-bimodule which is flat as a right S-module. Show that $E \otimes_R F$ is flat as a right S-module.

XVI.3:8. Let R be the ring of all continuous functions on the interval $[0,1]$, and E the R-module of all ''germs at 0'' of such functions; i.e., the R-module R/I, where I is the ideal of all functions zero in the neighborhood of 0. Show that E is a flat R-module. (This same ring and ideal appear in the more difficult Exercise III.4:2.)

XVI.3:9. Suppose S is a commutative integral domain, K is its field of fractions, and R is a subring of S having the same field of fractions.

(a) Show that every R-module homomorphism of S into R is given by multiplication by a member of R, and that the set of $r \in R$ such that multiplication by r carries S into R forms an ideal of R, which is the largest ideal of R that is also an ideal of S. This is called the *conductor ideal* of R in S.

(b) Determine the conductor ideal of $k[x]$ in $k[x, x^{-1}]$, and the conductor ideal of $k[x^2, x^3]$ in $k[x]$. Under what conditions on R and S will 1 belong to the conductor ideal?

(c) Show that if the identity map of S, regarded as a homomorphism of R-modules, factors through a free R-module, then $S = R$.

(d) Deduce that if S is finitely presented as an R-module (in particular, if R is Noetherian and S is finitely generated as an R-module) and is strictly larger than R, then S is not flat as an R-module.

XVI.3:10. Let k be a field, and $R = k\langle x, y\rangle$ the free associative k-algebra on indeterminates x and y, equivalently, the monoid algebra over k on the free monoid on x and y.

(a) Let P denote the right R-module presented by two generators α and β and the one relation

$\alpha x - \beta y = 0$. How that $\mathrm{Hom}_R(P, R) = 0$.

(b) Deduce that if $f: R \to S$ is a ring homomorphism such that either $f(x)$ or $f(y)$ is invertible in S, then S is not flat as a right R-module (under the induced module structure $s \cdot r = s\, f(r)$).

In particular, this shows that R cannot be embedded in a division ring that is flat as a right R-module, and also that the group algebra of the free group on x and y is not flat as a right R-module.

XVI.3:11. Within the division ring of quaternions, let

$R = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{Z}\}$,

$S = \{(a + bi + cj + dk)/2 \mid a, b, c, d \in \mathbf{Z},\ a \equiv b \equiv c \equiv d \pmod 2\}$,

$K = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{Q}\}$.

Clearly, R is a ring and K a division ring.

(a) Verify that S is also a ring.

(b) Show that K is flat both as a right R-module and as a right S-module.

(c) Show that S is not flat as a right R-module. (Suggestion: Look for analogs of the ideas of XVI.3:9.)

(d) Show that every right ideal of S is principal, and deduce that every right S-module which is torsion-free as an abelian group is flat.

Remark: From (c) and (d), we see that S is ''better behaved'' than R; e.g., S is a ''noncommutative principal right (and left) ideal domain'', while R is not. So S is commonly called the ''ring of integer quaternions'', while there is no special name for R.

***XVI.3:12.** (a) Show that if R is a commutative Noetherian ring, and P a finitely presented R-module, then there exists a homomorphism h of P into a free R-module F of finite rank such that any homomorphism of P into a free R-module factors through h.

(b) Deduce that the direct product of an (in general, infinite) family of flat R-modules over a commutative Noetherian ring is flat. (We already know this for direct products of finite families, since these are the same as direct sums.)

(c) To show that (b) fails for non-Noetherian R, let G be a monoid isomorphic to the monoid $[0, \infty)$ of nonnegative real numbers, but written multiplicatively as $\{x^r \mid r \in [0, \infty)\}$, let S be the monoid algebra kG, and let R be the factor-ring of S by the ideal generated by all x^r with $r > 1$. (One might write this sloppily as $k[x^{[0,1]}]$.) Show that a direct product of countably many copies of R is not flat. (Hint: The element $a = (x, x^{1/2}, x^{1/4}, \ldots)$ satisfies the relation $ax = 0$.)

(d) Prove versions of (a) and (b) for noncommutative R.

XVI.4:1. Let $f: R \to S$ be a ring homomorphism, let A be a right R-module, and let B be a left S-module. Establish a natural isomorphism $A \otimes_R B = A_S \otimes_S B$ as abelian groups. Describe the isomorphism and its inverse explicitly on generators of these tensor products if your method of obtaining the isomorphism does not do so.

XVI.5:1. Let R be a commutative ring, and E and F R-modules. It is easy to see that the construction of Lang's Corollary XVI.5.5 (p.628) gives a functorial homomorphism $\varphi_{E,F}: E^{\vee} \otimes F \to \mathrm{Hom}(E, F)$, without the assumption of that corollary that the modules be free of finite rank.

Characterize some of the following classes of modules. (Instructor should specify how many; e.g., ''two''.)

(a) Those E such that for all F, $\varphi_{E,F}$ is an isomorphism.

(b) Those F such that for all E, $\varphi_{E,F}$ is an isomorphism.

(c) Those F such that for all free modules E, $\varphi_{E,F}$ is an isomorphism.

(d), (e), ... Similar cases with ''an isomorphism'' replaced by ''one-to-one'' or ''onto'', and/or with other classes of modules, so long as you don't hand in two results with slightly varying hypotheses but essentially the same proofs.

XVI.6:1. Let A be a $\mathbf{Z}$-graded or $\mathbf{Z}/2\mathbf{Z}$-graded algebra, as in the last paragraph on p.631 of Lang.

(i) If the grading monoid is $\mathbf{Z}$, show that what Lang calls the ''super algebra A_{su}'' is actually isomorphic to the ''ordinary algebra A''.

(Suggestion: Take a polynomial ring $R[x]$, grade it so that x has degree 1, and determine the unique R-algebra isomorphism $R[x] \to R[x]_{\mathrm{su}}$ carrying x to x. This will involve multiplying homogeneous elements of each degree by an appropriate coefficient. Verify that these same coefficients give an isomorphism in the case of any $\mathbf{Z}$-graded algebra.)

(ii) On the other hand, show that if we grade the complex numbers by $\mathbf{Z}/2\mathbf{Z}$, letting $\mathbf{C}_0 = \mathbf{R}$ and $\mathbf{C}_1 = i\mathbf{R}$, then $\mathbf{C}_{\mathrm{su}}$ is not isomorphic to $\mathbf{C}$.

***XVI.8:1.** For E a module over a commutative ring R and n a positive integer, does $S^n E = 0 \Rightarrow \otimes^n E = 0$?

(This question was asked by Moss Sweedler. I succeeded in answering it a few years ago; but it has potential generalizations in the context of the representation theory of the symmetric group which could form an interesting research topic.)

XX.4:1. *(a) = XX:L20 (p.830). (Suggestion [> XX:L23]: Show that any ideal of $S^{-1}A$ has the form $S^{-1}J$ for an ideal J of A. Use the fact that J can be finitely presented as an A-module to show that any $S^{-1}A$-module homomorphism $f\colon S^{-1}J \to S^{-1}I$ is of the form $s^{-1}\bar{\varphi}$, where $s \in S$, and $\bar{\varphi}\colon S^{-1}J \to S^{-1}I$ is the map induced by an A-module homomorphism $\varphi\colon J \to I$. Then get the desired result using XX:L23.)

Parts (b) and (c) below refer to the statement of the exercise comprising part (a), but do not depend on it or one another. Part (d) depends on (a) and (c).

(b) (T.Y.Lam) Show that the conclusion of the above exercise remains true if the assumption ''A is Noetherian'' is replaced by the condition that the module I has no S-torsion; i.e., that no nonzero element of I is annihilated by an element of S.

*(c) Show that the result in question becomes false if neither the Noetherian condition of part (a) nor the no S-torsion condition of (b) is assumed. (Suggestion [> XX:L21(a)]: Let k be an algebraically closed field, and regard the polynomial ring $k[x,y]$ as a subring of the ring of k-valued functions in two k-valued variables, $k^{k\times k}$. Let A be the subring of $k^{k\times k}$ spanned by $k[x,y]$ and all functions of finite support, and let $I = k^{k\times k}$ regarded as an A-module. XX:L21(a) reduces the problem of showing I injective to the same problem for certain much smaller modules; get these cases with the help of the fact that the element of A having the value 1 at a single point and 0 elsewhere is idempotent, hence induces a direct product decomposition of A as a ring. Now let $S = k[x] - \{0\} \subseteq k[x,y] \subseteq A$, and get descriptions of $S^{-1}A$, and $S^{-1}I$. Show that if $S^{-1}I$ were injective, then multiplication by y would map it *onto* itself, but that it does not.)

*(d) [> §III.10] Give a version of the proof of (a) above that proceeds via the following three results: (i) if A is Noetherian, then a direct limit of injective A-modules is injective; (ii) for any commutative ring A, any A-module I, and any multiplicative set S, $S^{-1}I$ can be expressed as a direct limit of copies of I; (iii) if an $S^{-1}A$-module is injective as an A-module, it is injective as an $S^{-1}A$-module.

Deduce from (c) that the condition that A be Noetherian cannot be dropped from (i) above.

Notes on exercises connected with Lang's Appendix A2: Exercises I.1:1 above assumes that Appendix A2.1 was read before §I.1. If they are read in the reverse order, that can be considered an exercise for Appendix A2.1.

Exercises A2.2:1-4 below concern Zorn's Lemma, developed in Appendix 2.2 and in my handout on ''The Axiom of Choice, Zorn's Lemma and all that''. Since I introduce this material between sections I.6

and I.7 of Lang, most of the exercises below assume the material in the first part of Chapter I.

If Exercise A2.2:1 is not assigned, it should probably be discussed in class.

A2.2:1. Show the following facts. (Negative results should be shown by constructing counterexamples, and proving relevant properties of these if they are not obvious.)

(a) Every nontrivial finitely generated group G has a maximal proper subgroup. (This means a maximal element in the class of proper subgroups, partially ordered by inclusion.)

(b) Every nontrivial finitely generated group G has a maximal proper *normal* subgroup (a maximal member of the class of proper normal subgroups).

(c) A nontrivial finitely generated group G need not have a minimal nontrivial subgroup. (I.e., there exists a nontrivial finitely generated group G not having such a subgroup.)

(d) Every nontrivial finitely generated group G has a simple homomorphic image.

(e) A maximal proper subgroup of a group G need not be normal, and a maximal proper normal subgroup of G need not be a maximal proper subgroup of G.

(f) A nontrivial *non*-finitely-generated group G need not have a maximal proper subgroup, nor a maximal proper normal subgroup, nor a simple homomorphic image.

(Remark: The terms ''maximal proper subgroup'', ''minimal nontrivial subgroup'', etc. are often shortened to ''maximal subgroup'', ''minimal subgroup'', etc.. That is, since the properties of maximality and minimality in the class of *all* subgroups of G characterize subgroups that can be named much more easily, it is taken for granted that when one refers to maximality or minimality, one must be thinking of proper, respectively nontrivial, subgroups. But there are situations where such abbreviation can lead to confusion; so be cautious in using them. If you are going to be writing extensively about maximal proper subgroups and want to use this abbreviated term, you should begin by *saying* that ''maximal subgroup'' will be understood to mean ''maximal proper subgroup''.)

A2.2:2. [cf. A2.2:1]. (a) Does every nontrivial finitely generated semigroup have a simple homomorphic image? (A semigroup S is called *simple* if it is nontrivial, and every homomorphism from S to another semigroup is either an isomorphism, or is trivial, i.e., has one-element image.)

(b) If G is a group, will every nontrivial finitely generated G-set have a simple homomorphic image?

A2.2:3. Let X be a set. If $\leq$ and $\leq'$ are two partial orderings on X, we say that $\leq'$ is a *refinement* of $\leq$ if

$$(\forall\, x,y\in X)\ \ x\leq y\ \Rightarrow\ x\leq' y,$$

i.e., if, when we regard the relations $\leq$ and $\leq'$ as subsets of $X\times X$, the former is contained in the latter. Clearly, ''is a refinement of'' is a partial ordering on the set of partial orderings on X!

(a) Show that every partial ordering on X can be refined to a partial ordering *maximal* with respect to refinement.

(b) Show that every such maximal partial ordering is a total ordering.

(c) Is every partial ordering on X the *intersection* of some set of total orderings?

A2.2:4. For this exercise, we need the following definition and observations.

A *subdirect product* of a family of groups G_i $(i\in I)$ means a subgroup G of the direct product $\prod_I G_i$, whose projection to each G_i is *surjective*. (Precisely: the composite of the inclusion $G\to\prod_I G_i$ with each projection $\prod_I G_i\to G_j$ is surjective.) Given a group G, we say that G ''can be written as a subdirect product of'' a family of groups G_i if it is isomorphic to such a subgroup of their product. Note that in this situation, each G_i will be isomorphic to a factor-group G/N_i, and the intersection of these N_i will be $\{e\}$. Conversely, given G and any system of normal subgroups with trivial intersection, we get a representation of G as a subdirect product of the factor-groups G/N_i.

A group G is called *subdirectly irreducible* if the only representations of G as a subdirect product are those in which at least one of the maps $G \to G_i$ is an isomorphism.

(a) Show that G is subdirectly irreducible if and only if it has a *smallest nontrivial* normal subgroup (a nontrivial normal subgroup contained in all nontrivial normal subgroups).

(b) Show that if G is a group, x an element of G, and N a normal subgroup of G maximal for the property $x \notin N$, then G/N is subdirectly irreducible.

(c) Deduce that every group can be written as a subdirect product of a family of subdirectly irreducible groups.

(Exercise I.6:5 concerned some restricted cases of the above results. There, finiteness allowed one to work without Zorn's Lemma, and to express the conclusion in terms of embedding in a product of groups of smaller order.)

A2.2:5. Let G be a group. By a ''maximal abelian subgroup'' of G we understand a maximal member of the class of abelian subgroups; not necessarily maximal as a subgroup of G. Recall also that the *centralizer* of a subset $X \subseteq G$ means $\{g \in G \mid (\forall\, x \in X)\ xg = gx\}$.

(a) Show that every abelian subgroup of G is contained in a maximal abelian subgroup.

(b) Show that the maximal abelian subgroups of G are precisely those subgroups of G that are their own centralizers.

(c) Show that for a subgroup (in fact, a subset) A of G, the following three conditions are equivalent: (i) A is the intersection of a nonempty set of maximal abelian subgroups of G. (ii) A is the centralizer of some subset of G containing A. (iii) A is an abelian subgroup of G, and for every element $g \in G$ not in A, there is an element $h \in G$ which commutes with all elements of A, but not with g. (Note: the next part, (d) is an easy consequence of (c). But if you are having trouble proving one of the implications needed for (c), you might try to work out a direct proof of (d), then see whether the argument you arrive at can be modified to complete your proof of (c).)

(d) Show that the *center* of G is the intersection of all maximal abelian subgroups of G.

A2.4:1. Let A be a partially ordered set. Show that the partial ordering of A can be refined (in the sense of A2.2:3) to a well-ordering if and only if every nonempty subset of A has an element minimal with respect to the given ordering. (Hint: Mimic the proof of Theorem A2.4:1.)

Note on A2:L13 (i.e., Exercise 13 at the end of Appendix 2, p.893). Hint: The set of maps from X to Y is often denoted Y^X. Think ''laws of exponents'', then try to justify the argument precisely.

INDEX TO DISCUSSION OF LANG'S EXERCISES IN THIS *COMPANION*

mostly in the above collection of exercises, but occasionally elsewhere
(excluding errata that apply only to earlier printings, for which see ''Errata'' section)

Exercises to Chapter I, pp.75-82: #3 clarified in I.3:1. Note on #4 at end of exercises on §I.3. #5 discussed and generalized in I.3:2. #6 incorporated into I.6:4(a). #7 incorporated into I.5:1. #15 and #16 incorporated into I.5:4. #24 incorporated into I.6:1. #38(d) generalized in I.5:7. In #44 an assumption can be deleted, as noted at end of exercises on §I.2. #47 incorporated into I.5:6. #57: Examples at end clarified at end of exercises on §I.5.

Exercises to Chapter II, pp.114-116: #1 subsumed by II.2:1. #3 incorporated into II.4:2. #5 clarified at end of exercises on §II.5. #9 belongs in Chapter IV but done in Companion, as noted at end of exercises on §II.1. Clarification of #12 and cross-reference from #13-19 to III:L11-13 noted at end of exercises on §II.1

Exercises to Chapter III, pp.165-171: Hint to #10 given at end of exercises on §III.1. Note that #5-#8 can go with §I.7 after exercises for that section. #6 **corrected** after exercises on §III.5. #14 clarified after exercises on §III.7. #16 discussed (''trivial or misstated'') after exercises on §III.9; related questions given as III.10:1-2.

Exercises to Chapter IV, pp.213-220: #8 and #9 incorporated into II.3:1. Notation of #12 clarified at end of exercises on §IV.6.

Exercises to Chapter V, pp.253-259: Comments on #17 and #21, and hint to #28, given after exercises for this chapter. #24 is covered in discussion *Examples involving inseparable extensions* (this Companion, note to p.252 of Lang).

Exercises to Chapter VI, pp.320-332: #6 clarified in discussion following exercises to §VI.6. #8 generalized and discussed in VI.2:1. Converse to #9 given as VI.2:5. #10, #14, #16 clarified following exercises for VI.2. #25 generalized in VI.14:2. Strengthened version of #26 asked for in VI.14:1. Suggestion on #29 following exercises to §VI.6.

Exercises to Chapter VIII, pp.374-375: #1 clarified/criticized after exercises on §VIII.1. #6 **corrected** after exercises on §VIII.1.

Exercises to Chapter XIII, pp.545-552: #25 incorporated into XIII.4:3. Possible converse to #26 given as XIII.4:1. #32, with different approach, given as VI.5:1; still another approach noted in *Further observations on linear independence of characters* (this Companion, note to p.284 of Lang).

Exercises to Chapter XIV, pp.567-570: #10 incorporated, with clarification, in XIV.3:1.

Exercises to Chapter XVI, pp.637-639: #6 generalized to bimodules in XVI.3:7. #13 developed in detail (with some **corrections** noted) in *Further criteria for flatness* (this Companion, note to p.613 of Lang), and alternative argument to one implication given as XVI.3:3.

Exercises to Chapter XX, pp.826-832: #20 incorporated into XX.4:1.

Exercises to Appendix 2, pp.892-893: Hint to #13 given after exercises to that Appendix.