Math 250A, Fall 2004
Problems due October 5, 2004

The problems this week were from Lang's "Algebra, Chapter I."

24. We basically know already that groups of order p^2 are abelian. Indeed, p-groups have non-trivial centers, and a group mod its center can be cyclic only if the group is abelian. Let G be a group of order p^2. If there's an element of order p^2, it's cyclic. If not, the group is killed by p and can therefore be regarded as a vector space over the field k consisting of integers mod p. Vector spaces are determined up to isomorphism by their dimensions; here, the dimension must be 2 because a vector space of dimension n over k has p^n elements. Summary: G can be cyclic or non-cyclic, but it's determined uniquely up to isomorphism once we know which type we're dealing with.

25. For (a), note that G/Z cannot be cyclic and that Z must be non-trivial. Hence G/Z is a non-cyclic group of order p^2 and is therefore isomorphic to $C \times C$ by the previous problem. For (b), we consider a subgroup N of G that has p^2 elements. It's normal because its index in G is the smallest prime dividing $\#G$. It's abelian because it has order p^2. The group ZN is then an abelian subgroup of G whose order is $p^3/\#(Z \cap N)$. Since G is non-abelian, $Z \cap N$ must be of order > 1. Hence its order is p, so that N contains Z. Finally, for c we note that G must have a subgroup H of order p^2. To construct one, we take an element of order p in the center of G, consider G/N, where N is the cyclic group generated by this element, and pull back to G a subgroup of G/N of order p. The subgroup H will be normal because its index, p, is the smallest prime dividing the order of G. The group H is isomorphic to $C \times C$, as required, because it's an abelian group killed by p (and thus a vector space over the field with p elements).

26a. [Part (b) clearly follows from part (a).] We note that both the p- and the q-Sylow subgroups of G are normal. This makes G the product of those groups by problem 13 (HW #2). Because p and q are primes, the two Sylow groups are cyclic. Because p and q are relatively prime, the product of cyclic groups of those orders is again cyclic.

28. Once you know that there's a normal Sylow subgroup, you know that the group is solvable because groups of orders p^2 and q are solvable. If the p-Sylow is not normal, we have $q \equiv 1 \bmod p$. This implies that $p \not\equiv 1 \bmod q$, so the number of q-Sylows must be 1 or p^2. In the latter case, we have $p^2 \equiv 1 \bmod q$, and thus $p \equiv -1 \bmod q$. We seem to have $p = 2$ and $q = 3$ when the two congruences $q \equiv 1 \bmod p$ and $p \equiv -1 \bmod q$ are true. To summarize, if one of the two Sylows is not normal, G is a group of order 12 in which there are three 2-Sylows and four 3-Sylows. What's wrong with this is that G will have eight elements of order 3: two from each 3-Sylow. Every 2-Sylow must lie in the complement of the set of elements of order 3. Thus complement has four elements, so we conclude that the 2-Sylow is unique in a situation when we posited three of them.

29. Assume that neither the p- nor the q-Sylow subgroup is normal. The number of p-Sylows is either q or $2q$, and similarly the other way around. If the number of p-Sylows is q and vice versa, then p is 1 mod q and also q is 1 mod p. This is impossible because then $p > q$ and $q > p$ simultaneously. If the number of p-Sylows is $2q$ and the number of q-Sylows is $2p$, then there are $2p(q-1)$ elements of order q and $2q(p-1)$ elements of order p. We then have

$$2p(q-1) + 2q(p-1) \leq 2pq - 2$$

since there are at least two elements of the group that are of order dividing 2. I get from this something like $pq < p + q$, which is pretty absurd. (If p is the bigger prime, then $pq < 2p$, so $q < 2$.) The remaining possibility is that, perhaps after switching p and q, there are $2q$ p-Sylows and p q-Sylows. Then $p \equiv 1 \bmod q$ and $2q \equiv 1 \bmod p$. I seem to get into a contradiction in this situation as well: Clearly, p is bigger than q and $2q > p$. If $2q - 1 = tp$, with t an integer, t must be 1 because $q > p$. This gives $p \equiv -1 \bmod q$, which is impossible because p is 1 mod q.

30. Part (b) is a special case of problem 28. Part (a) was done in class—the point is that the 5-Sylow is normal because the number of 5-Sylows is a divisor of 8 that is 1 mod 5.

39. It suffices to show that we can map $(1, 2, \ldots, n-2)$ to an arbitrary tuple $x_1, \ldots, x_{n-2}$ of distinct numbers in $\{1, \ldots, n\}$ by an element of $\mathbf{A}_n$. Let σ be the permutation sending 1 to x_1, 2 to x_2, etc. If σ is even, great. If not, we use $\sigma(n-1\, n)$ instead.

40. For (a), the kernel of the left-translation map $\mathbf{A}_n \to \mathrm{Perm}(\mathbf{A}_n/H)$ is the intersection of the conjugates of H. For $n = 3$, $\mathbf{A}_n$ has order 3, and H has order 1, so the kernel is trivial. For $n = 4$, maybe one has to see by inspection that there's no normal subgroup of order 3 in $\mathbf{A}_n$. (The subgroups of order 3 are generated by 3-cycles, so this should be pretty clear.) For $n \leq 5$, the triviality of the kernel follows from the simplicity of $\mathbf{A}_n$, which we proved in class. We find in all cases that the map $\mathbf{A}_n \to \mathrm{Perm}(\mathbf{A}_n/H)$ is an injection, which identifies $\mathbf{A}_n$ with a subgroup of index 2 in $\mathrm{Perm}(\mathbf{A}_n/H) \approx \mathbf{A}_n$. This subgroup contains all 3-cycles of $\mathrm{Perm}(\mathbf{A}_n/H)$ since it contains all squares of elements of $\mathrm{Perm}(\mathbf{A}_n/H)$. We've seen, though, that $\mathbf{A}_n$ is generated by its 3-cycles if $n \geq 5$, so we conclude that the image of $\mathbf{A}_n$ in $\mathrm{Perm}(\mathbf{A}_n/H)$ is the alternating subgroup of $\mathrm{Perm}(\mathbf{A}_n/H$ at least when $n \geq 5$. For $n = 3$ and $n = 4$, we might have to check explicitly that here is only one possible subgroup of index 2 in $\mathbf{S}_n$.

Part (a) establishes an isomorphism $\alpha : \mathbf{A}_n \xrightarrow{\sim} \mathrm{Alt}(\mathbf{A}_n/H)$, where $\mathrm{Alt}(\mathbf{A}_n/H)$ is the alternating subgroup of $\mathrm{Perm}(\mathbf{A}_n/H)$. Make a bijection between $\mathbf{A}_n/H$ and $\{1, \ldots, n\}$ that sends the coset H to the letter "1". This bijection yields an isomorphism $\beta : \mathrm{Alt}(\mathbf{A}_n/H) \approx \mathbf{A}_n$. The composite $\beta \circ \alpha$ is an automorphism of $\mathbf{A}_n$. The first map, α, takes H to the group of elements of $\mathrm{Alt}(\mathbf{A}_n/H)$ that fix H. The map β takes this latter group to H_1, the group of elements of $\mathbf{A}_n$ that fix 1. The composite maps H to H_1. Note finally that inner automorphisms of $\mathbf{S}_n$ permute the various subgroups H_i of $\mathbf{A}_n$. Hence if H is not an H_i, the automorphism $\beta\alpha$ of $\mathbf{A}_n$ does not come from an inner automorphism of $\mathbf{S}_n$. This is the point that is needed in the next problem.

41. It's clear from the context that Lang is talking about 5-Sylow subgroups. The number of 5-Sylows in a group of order 60 is 1 mod 5 and is a divisor of 12. There are thus six 5-Sylows if there is more than 1. In a simple group of order 60, there are no normal subgroups of order 5; thus there are six 5-Sylow subgroups. The conjugation map $H \to \mathrm{Perm}\, S$, where S is the set of 5-Sylow subgroups, must be an embedding because H has no non-trivial normal subgroups. Notice that H is generated by its elements of order 3 since the subgroup of H generated by these elements is normal and not the identity group. These elements map to even permutations of S because the cubes of their signs are 1, so the signs must be 1, rather than -1. Hence H gets embedded into $\mathbf{A}_6$ as a subgroup of index 6. By exercise 40, there is an automorphism of $\mathbf{A}_6$ that maps H onto the subgroup H_1 of $\mathbf{A}_6$. To see that this automorphism is not induced from an inner automorphism of $\mathbf{S}_6$, we have to check that H is not one of the subgroups H_i of $\mathbf{A}_6$. But each H_i fixes one of the six letters on which $\mathbf{A}_6$ acts. However, H fixes none of the six 5-Sylow subgroups of H (i.e., no element of S). In fact, the Sylow theorems say in particular that the action of H on S is transitive: the Sylows are all conjugate to each other.

46. To prove that **PRIM 1** implies **PRIM 2**, we suppose that there are no non-trivial G-stable partitions of the G-set S, and let H be the stabilizer of $s \in S$. Clearly, H is a proper subgroup of G because S has more than two elements. In fact, since G operates transitively on S, the map $g \mapsto gs$ induces a bijection of G-sets $G/H \xrightarrow{\sim} S$; the index $(G : H)$ is the cardinality of S, which is at least 2. To say that H is maximal is to say that there is no subgroup of G between H and G. To see that H is maximal, suppose that there is an H' strictly between H and G. Then the subsets of S of the form $gH' \cdot s$ with $g \in G$ (or, really, $g \in G/H'$) form a non-trivial G-stable partition of S.

In the other direction, suppose that there is a non-trivial G-stable partition of S. (We suppose then that **PRIM 1** is false.) Let s be an element of S and let $S_0 \subseteq S$ be that subset of S that contains s and is part of the partition. Then S_0 is bigger than $\{s\}$ but smaller than S. If H is the stabilizer of s, then H is contained in the stabilizer H' of the set S_0: the group of $g \in G$ that map S_0 to itself. The index $(G : H')$ is the number of elements of the partition, whereas the index $(G : H)$ is the number of elements of S. We have $1 < (G : H') < (G : H)$ because the partition was supposed to be non-trivial. Hence H is not a maximal subgroup of G.

47. In the situation of this problem, the "transitive" hypothesis means that we can replace S by G/H. The fidelity means that the intersection of the conjugates of H is the identity subgroup of G. The action is doubly transitive if G sends each pair of distinct elements of G/H to any arbitrary pair of distinct elements of G/H. Since G acts transitively on G/H, we can assume that the first entry in both the source and target pair is the identity coset H. The double transitivity condition means simply that we can send (H, aH) to (H, bH) whenever a and b are elements of G in the complement of H. If an element of G sends H to H, it must be in H, so we are saying that H can send an arbitrary aH ($a \notin H$) to an arbitrary bH ($b \notin H$). This gives part (a).

Suppose now that G is as in the general statement of the problem and that G acts doubly transitively on S. Take distinct elements a and b in S and find $g \in G$ that takes (a, b) to (b, a). Then G acts on the 2-element set $\{a, b\}$ as an involution, so that G has even order. Some power of G then has order 2, which implies in particular that G has some elements of order 2. I claim that not all elements of G with order 2 lie in H. Indeed, the set of elements of order 2 is stable by conjugation. If all elements of G of order 2 were in H, then they'd all be in the intersection of the conjugates of H. However, this intersection is trivial because G was assumed to act *faithfully* on S. Let t now be an element of order 2 that is not in H. Suppose that $g \in G$ is also not in H. Then, by part (a), we know that there is an $h \in H$ such that $htH = gH$. It follows that g lies in HTH, where $T = \{e, t\}$ is the subgroup of G generated by t. If, on the other hand, g does lie in H, then $g = gee$ also lies in HTH. Thus $G = HTH$.

Suppose, conversely, that $G = HTH$, where $T = \{e, t\}$, t is of order 2, and t isn't in H. The cosets in G/H other than the identity coset are all of the form htH with $h \in H$. It is obvious that H acts transitively on the set of these cosets, so G acts doubly transitively, as we wanted.

For the formula with $n(n-1)$, we consider the action of G on $S \times S$, which has cardinality n^2. (The integer $n = (G : H)$ is also the size of S.) There are two orbits: the diagonal and the set of non-diagonal elements. The latter set is permuted transitively by G; the number of elements in it is $\#(G)/d$ because d is the order of the stabilizer of any one of the elements. We get $n^2 = n + \#(G)/d$, which gives the desired formula.

Finally, we are to prove that H is maximal if G acts doubly transitively. We prove the contrapositive. Suppose, then, that we have $H \subset K \subset G$ where K is a proper subgroup of G that is bigger than H. Take $k \in K$, $k \notin H$ and $g \in G$, $g \notin K$. The two elements gs and ks of S lie in the complement of $\{s\}$ but are not linked by an element of H. Indeed, if $gs = hks$, then $g^{-1}hk \in H$ forces $g \in K$, which is impossible by our choice of g. Hence G does not act doubly transitively on S (because of part (a)).

48. Part (a) is a re-hash of 19(b), since we suppose that there is only one orbit. For part (b), we note that G acts doubly transitively on S if and only if there are exactly two orbits for the action of G on $S \times S$: the diagonal (consisting of pairs (s,s)) and the complement of the diagonal. Hence G is doubly transitive if and only if $2\#(G) = \sum_{x \in G} F(x)$, where $F(x)$ is the number of fixed points of x acting on $S \times S$. One sees easily that $F(x) = f(x)^2$; the desired formula now follows from this.

50. We're trying to show that products exist in the category $\mathcal{C}$ of "Z-abelian groups," abelian groups furnished with maps to Z. Two such objects might be $f \colon X \to Z$ and $g \colon Y \to Z$, to use the book's notation. The abelian group $P := X \times_Z Y$, as defined in the problem, is naturally a Z-group: we endow it with the map $h \colon P \to Z$ sending (x,y) to $f(x)$ (which is also $g(y)$. It comes equipped with $p_1 \colon P \to X$ and $p_2 \colon P \to Y$, the maps sending (x,y) to x and y, respectively. These are really maps in the category of Z-groups because we have, trivially, $f \circ p_1 = g \circ p_2 = h$.

To show that $h \colon P \to Z$ is really a product is to check that a certain map is a bijection. Namely, suppose that $\alpha \colon A \to Z$ is an object in the category of Z-abelian groups. For short, we can write $\mathrm{Mor}_{\mathcal{C}}(A,P)$ for the set of homomorphisms $\varphi \colon A \to P$ such that $h \circ \varphi = \alpha$; we use a similar abbreviation in other, analogous, contexts. There's a natural map

$$\mathrm{Mor}_{\mathcal{C}}(A,P) \to \mathrm{Mor}_{\mathcal{C}}(A,X) \times \mathrm{Mor}_{\mathcal{C}}(A,Y)$$

gotten by composing with p_1 and p_2. What has to be shown is that this map is a bijection of sets. A convenient way to do this is to find a map in the opposite direction and to check that the composites of the two maps are the identity maps of $\mathrm{Mor}_{\mathcal{C}}(A,P)$ and $\mathrm{Mor}_{\mathcal{C}}(A,X) \times \mathrm{Mor}_{\mathcal{C}}(A,Y)$, respectively. Given $\psi \in \mathrm{Mor}_{\mathcal{C}}(A,X)$ and $\theta \in \mathrm{Mor}_{\mathcal{C}}(A,Y)$, we consider the map $A \to X \times Y$ given by $a \mapsto (\psi(a), \theta(a))$. Because $f \circ \psi = g \circ \theta = \alpha$, $(\psi(a), \theta(a))$ lies in $X \times_Z Y$. Also, $h((\psi(a), \theta(a)) = f(\psi(a)) = g(\theta(a)) = \alpha(a)$, so we are really constructing a map $A \to P$ in the category $\mathcal{C}$. I won't perform the check that this construction is inverse to the construction $\mathrm{Mor}_{\mathcal{C}}(A,P) \to \mathrm{Mor}_{\mathcal{C}}(A,X) \times \mathrm{Mor}_{\mathcal{C}}(A,Y)$ gotten by composing with p_1 and p_2.

Lang wants us to show that the pullback of a surjective homomorphism is surjective. Here, there's an asymmetric perspective. He imagines that a map $f \colon X \to Z$ is somehow given and that one pulls back this map by $g \colon Y \to Z$ to obtain $p_2 \colon P \to Y$. We want to show that p_2 is surjective if f is surjective. Given $y \in Y$, we use the surjectivity of f to find $x \in X$ such that $f(x) = g(y)$. The point $(x,y) \in X \times Y$ is actually then in $X \times_Z Y$; its second coordinate (which is the image of (x,y) under p_2) is y. Since y is an arbitrary element of Y, we see that p_2 is surjective, as required.

52. This problem is like #50, but with all the arrows reversed. When Lang writes that f and g are "as above," he means "as above with arrows reversed." We are given $f \colon Z \to X$ and $g \colon Z \to Y$. We form

$$X \oplus_Z Y := (X \oplus Y)/\{\, (f(z), -g(z)) \mid z \in Z \,\}.$$

There's a natural map $Z \to X \oplus_Z Y$ given by $z \mapsto \overline{(f(z),0)} = \overline{(0,g(z))}$, where we use $\overline{}$ for "image in $X \oplus_Z Y$." We have $X \to X \oplus_Z Y$ given by $x \mapsto \overline{(x,0)}$, and there's a similar map with X replaced by Y. The composite of $X \to X \oplus_Z Y$ and $f \colon Z \to X$ is the map $Z \to X \oplus_Z Y$ that we constructed, so we really have a morphism in the category of "abelian groups X together with a map from Z to X," i.e., the category of homomorphisms $f \colon Z \to X$ (Z fixed but X varying). By reasoning similar to that of problem 50, we show that $Z \to X \oplus_Z Y$, with the maps $X \to X \oplus_Z Y$, $Y \to X \oplus_Z Y$, is really the coproduct of f and g. The injectivity statement is the following: if f (say) is injective, then $Y \to X \oplus_Z Y$ is injective. To show this, suppose that $y \in Y$ is in the kernel of $Y \to X \oplus_Z Y$. Then $(0, y) = (f(z), -g(z))$ for some z. Because f is injective, $z = 0$, which implies that $y = g(z) = 0$.