

# Math 153: HW Hints

Rich Schwartz

October 16, 2009

**2.3.2:**  $(ab)^n = ab(ab)^{n-1} =^* aba^{n-1}b^{n-1} = aa^{n-1}bb^{n-1} = a^n b^n$ . The starred equality is induction.

**2.3.3:**  $abab = aabb$ . Cancel to get  $ab = ba$ .

**2.3.4:** Suppose the exponents are  $k, k+1, k+2$ . Then

$$aa^k b^k b = a^{k+1} b^{k+1} = (ab)^{k+1} = ab(ab)^k = aba^k b^k.$$

Cancel the  $a$  on the left:

$$(a^k b^k)b = b(a^k b^k).$$

So  $b$  commutes with  $a^k b^k$ . But  $b$  also commutes with  $b^{-k}$ . Hence  $b$  commutes with  $a^k$ . Using  $k+1$  in place of  $k$ , we see that  $b$  commutes with  $a^{k+1}$ . So,  $b$  commutes with both  $g = a^k$  and  $h = a^{k+1}$ . But then  $b$  commutes with  $g^{-1}h = a$ .

**2.3.8:** For each  $g$  there is some  $N_g$  such that  $g^{N_g} = e$ . Let  $N$  be the product of all  $N_g$ . This  $N$  works. Alternatively, if you know more, you could let  $N = o(G)$ .

**2.3.9:** If  $G$  has order 3 then two of the elements of  $G$  are  $e$  and  $a$ . If  $a = a^{-1}$ , then there is some other element  $b$  with no inverse. Hence  $G = \{e, a, a^{-1}\}$ . But then all elements obviously commute. When  $G$  has order 4, there are elements  $a$  and  $b$  such that  $e$  and  $a$  and  $b$  are three elements of  $G$ , and  $b \neq a^{-1}$ . But then  $ab$  is none of the elements  $e, a, b$ . Hence  $G = \{e, a, b, ab\}$ . A case-by-case argument shows that  $ba = ab$ . The other 3 possibilities for  $ba$  lead to contradictions. When  $G$  has order 5 we could use the fact that

$G$  has prime order and hence is cyclic. Here's an alternate argument. If all elements of  $G$  have order 2 then  $G$  is abelian. (See problem 10.) Hence,  $G$  has some element  $a$  of order at least 3. If  $G$  is not cyclic then there is some  $b \in G$ , not a power of  $a$ . But then  $e, a, a^2, b, ab$  are all the elements of  $G$  and  $e, a, a^2, b, ba$  are also all the elements of  $G$ . But this forces  $ab = ba$ . From here, it's easy to finish.

**2.3.10:**  $abab = e$ . Left and right multiply to get  $ba = a^{-1}b^{-1} = ab$ .

**2.3.11:** Note that  $e$  is its own inverse. If no other element is its own inverse, we can list the elements of  $G$  as

$$e, g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_k, g_k^{-1}.$$

But then  $G$  has an odd number of elements, contradiction.

**2.5.2:** If  $G$  has an element of infinite order, then  $G$  has a subgroup  $H$  that is isomorphic to  $\mathbf{Z}$ . So, it suffices to prove that the intersection of all subgroups of  $\mathbf{Z}$  is just  $\{0\}$ . Choose some nonzero  $n \in \mathbf{Z}$ . The subgroup  $(n+1)\mathbf{Z}$ , all multiples of  $n+1$ , does not contain  $n$ . Hence, the intersection of all subgroups does not contain  $n$ . But  $n$  is arbitrary.

**2.5.12:** Argue by contradiction. If  $H \cap K$  has infinite index in  $G$  then consider an infinite list  $g_1, g_2, \dots$  of inequivalent elements. Since there are only finitely many possibilities, it must happen that we can find two indices  $i$  and  $j$  such that  $g_i \equiv g_j \pmod{H}$  and  $g_i \equiv g_j \pmod{K}$ . But then  $g_i g_j^{-1} \in H \cap K$ , contradiction. We can take

$$\max(i, h) < i_G(H)i_G(K) + 1.$$

This gives the bound

$$i_G(H \cap K) \leq i_G(H)i_G(K).$$

**2.5.14:** Closure under compositions  $abh = ahb = hab$ . Inverses are similar.

**2.6.1:**  $HaHe$  is a coset containing  $Ha$ . So,  $HaHe = Ha$ . Hence

$$aH \subset HaH = Ha.$$

In short,  $aH \subset Ha$  for any  $a$ . But then  $aHa^{-1} \subset H$  for all  $a$ . This is equivalent to normality.

**2.6.4:** Consider  $a \in N_1 \cap N_2$  and  $g \in G$ . Then  $gag^{-1}$  lies in  $N_1$  because  $N_1$  is normal and in  $N_2$  because  $N_2$  is normal. Hence  $gag^{-1} \in N_1 \cap N_2$ .

**2.6.8:** Let  $G = A(\mathbf{Z})$ . Let  $H$  be the set of permutations that fix the negative numbers. Let  $h$  be the map  $h(x) = x - 1$ . Then  $h^{-1}Gh$  fixes all numbers less than 1.

**2.6.11:**  $NMa = NaM = aNM$ .

**2.7.2:**  $\phi(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \phi(a)\phi(b)$ . Hence  $\phi$  is a homomorphism. A cancellation argument shows that  $g$  is one-to-one. Finally  $\phi(g^{-1}ag) = a$  for any  $a \in G$ , showing that  $\phi$  is onto.

**2.7.3:** Consider the map  $\phi(x) = x^n$ . By the pidgeonhole principle, it suffices to show that  $\phi$  is injective. Suppose that  $x^n = y^n$ . Since  $n$  is relatively prime to  $o(G)$ , we can find some  $m$  such that  $mn \equiv 1 \pmod{o(G)}$ . But then  $x = (x^n)^m = (y^n)^m = y$ .

**2.7.5:** (a) A typical element of  $G'$  has the form

$$w = (x_1y_1x_1^{-1}y_1^{-1})\dots(x_ky_kx_k^{-1}y_k^{-1})$$

Then

$$gwg^{-1} = gx_1g^{-1}gy_1g^{-1}\dots = X_1Y_1X_1^{-1}Y_1^{-1}X_2Y_2X_2^{-1}Y_2^{-1}\dots,$$

where  $X_j = gx_jg^{-1}$  and  $Y_j = gy_jg^{-1}$ . This shows that  $G'$  is normal.

(b) To show that  $G/G'$  is abelian, we must show that  $xyG' = yxG'$ . But this is equivalent to  $x^{-1}y^{-1}xyG' = G'$ , a true statement by definition of  $G'$ .

(c) Consider the map  $\phi : G \rightarrow G/N$ . Here  $N$  is the kernel of  $\phi$ . But  $\phi(xy x^{-1}y^{-1}) = \phi(x)\phi(y)(\phi(x))^{-1}(\phi(y))^{-1} = e$  because the image of  $\phi$  is abelian. This shows that the elements generating  $G'$  lie in the kernel. Hence  $G'$  lies in the kernel as well.

(d) Consider the map  $\phi : G \rightarrow G/G'$ . All subgroups of  $G/G'$  are normal

because  $G/G'$  is abelian. But  $H = \phi^{-1}(M)$  for some subgroup  $M$  of  $G/G'$ . The inverse image of a normal subgroup is normal, so that  $H$  is also normal.

**2.7.10:** The case when some element has order 9 is easy. If all elements have order 3, then  $G$  has 4 subgroups of order 3, namely  $\{e, a_j, a_j^{-1}\}$  for  $j = 1, 2, 3, 4$ . Call these subgroups  $H_1, H_2, H_3, H_4$ . Each  $g \in G$  gives a permutation of these 4 subgroups:  $H_j$  is mapped to  $gH_jg^{-1}$ . This gives us a homomorphism from  $G$  into  $S_4$ . Since 9 does not divide  $4!$ , this homomorphism has nontrivial kernel. So, there is some  $g$  such that  $gH_jg^{-1} = H_j$ . So, conjugation by  $g$  permutes the elements  $\{e, a_j, a_j^{-1}\}$ . Since  $g$  has order 3, the only possibility is that  $g$  commutes with these elements. We can assume that  $g \in H_1$ . But then all elements of  $H_1$  commute with all elements of  $H_2$ . Then  $G = H_1H_2$ , and from here it is obvious that  $G$  is abelian.

**2.7.12:**  $NaNb = Nab = Nba = NbNa$ .

**2.7.15:** Define  $\phi(a + bi) = |a + bi| = \sqrt{a^2 + b^2}$ , show this is an onto homomorphism, and then use the isomorphism theorem.

**2.8.3:**  $gT(N)g^{-1} = T(T^{-1}(g)NT^{-1}(g)) = T(N)$  for all  $g \in G$ .

**2.8.5:** Let  $I$  be an inner automorphism, conjugation by  $a$ , and let  $J$  be any automorphism. We compute

$$JIJ^{-1}(g) = J(aJ^{-1}(g)a^{-1}) = J(a)JJ^{-1}(g)J(a^{-1}) = bgb^{-1},$$

where  $b = J(a)$ . So,  $JIJ^{-1}$  is another inner automorphism, namely conjugation by  $b$ .

**2.8.6:** All nontrivial elements of  $G$  have order 2 and the product of any 2 of them is the third. Write  $G = \{e, a_1, a_2, a_3\}$ . Any automorphism of  $G$  permutes  $\{a_1, a_2, a_3\}$ . This gives a homomorphism from  $\mathcal{A}(G)$  to  $S_3$ . This is certainly injective. Our description of the group law, which was completely symmetric in the three nontrivial elements, shows that one can find an automorphism permuting  $\{a_1, a_2, a_3\}$  any way we like.

**2.8.11:** Suppose that  $T(g) = g^{-1}$  for all  $g$ . Then

$$x^{-1}y^{-1} = T(x)T(y) = T(xy) = (xy)^{-1} = y^{-1}x^{-1}.$$

This shows that  $x$  and  $y$  commute. So, let's show that  $T(g) = g^{-1}$  for all  $g$ . Note that this is true when  $g = a^{-1}T(a)$ . So, we need to show that every  $g$  can be written this way. Define  $\phi : G \rightarrow G$  by the rule  $\phi(a) = a^{-1}T(a)$ . If  $\phi(a) = \phi(b)$ , then  $a^{-1}T(a) = b^{-1}T(b)$ , which implies that  $T(ba^{-1}) = ba^{-1}$ . But then  $ba^{-1} = e$  and  $a = b$ . So  $\phi$  is injective. By the pigeonhole principle,  $\phi$  is also surjective. This does it.

**2.8.17:** We just show that  $T(g)$  commutes with everything when  $g \in Z$ . To show that  $T(g)h = hT(g)$ , note that

$$T^{-1}(T(g)h) = gT^{-1}(h) = T^{-1}(h)g = T^{-1}(hT(g)).$$

Since  $T^{-1}$  is injective, we have  $T(g)h = hT(g)$ .

**2.9.5:**  $G$  must have a subgroup of order  $p$ , because otherwise  $G$  would be cyclic. Let  $H$  be such a subgroup. Consider the map  $G \rightarrow A(G/H)$ . Since  $p^2$  does not divide  $p!$ , there is a nontrivial normal subgroup  $N \subset H$ . But then  $N = H$  because  $H$  has prime order.

**2.9.6:** Given  $g \in G$  define  $T : N \rightarrow N$  by the formula  $T(a) = gag^{-1}$ . Then  $T$  fixes  $e$  and permutes the remaining  $p - 1$  elements of  $N$ . In this way, we think of  $T$  as an element of  $S_{p-1}$ . But then  $o(T)$ , the order of  $T$ , divides  $(p - 1)!$ . On the other hand,  $g$  has order  $p$  so  $o(T)$  divides  $p$ . If  $o(T) \neq 1$  then  $o(T) = p$ . But  $p$  does not divide  $(p - 1)!$ . Hence  $o(T) = 1$ . But then  $T$  fixes all elements of  $N$ . But then  $g$  commutes with all elements of  $N$ . Since  $g$  is arbitrary, we see that all elements of  $G$  commute with all element of  $N$ .

**2.9.8:** If all elements of  $G$  have order  $2p$  then  $G$  is cyclic. This case is easy. If all elements of  $G$  have order 2 then  $G$  is abelian by a previous problem. Then Cauchy's theorem gives an element of order  $p$ , a contradiction. So,  $G$  must have an element of order  $p$ . Let  $H$  be the subgroup generated by this element. Since  $o(H) = p$ , we have  $i_G(H) = 2$ . But any subgroup of index 2 is normal.