

## HW 4 Solutions

May 2, 2009

**Chapter 3.1 Exercise 3:** Let  $A$  be an abelian group and let  $B$  be a subgroup of  $A$ . Prove that  $A/B$  is abelian. Give an example of a non-abelian group  $G$  containing a proper normal subgroup  $N$  such that  $G/N$  is abelian.

**Solution:** First off, all subgroups of an abelian group are normal, so  $A/B$  is well defined. Now given two cosets  $g_1B$  and  $g_2B$  that are elements of  $A/B$  we have  $g_1B \cdot g_2B = g_1g_2B \cdot B$  by the normality of  $B$  in  $A$ , but furthermore, this is equal to  $g_2g_1B \cdot B$  because  $A$  is abelian. But  $g_2g_1B \cdot B = g_2B \cdot g_1B$  again by the normality of  $B$  and this is precisely  $g_2B \cdot g_1B$ . So  $A/B$  is abelian.

For a simple example, let the group be  $S_3$  and let the proper normal subgroup  $N$  be the group generated by all 3-cycles. This group is of order 3 and consists of all the 3-cycles and the identity. It is normal, since conjugating an element of  $S_3$  preserves its cycle structure. Now  $S_3/N$  must be a group of order two. There is only one isomorphism class of groups with two elements, and that is  $\mathbb{Z}/2$  which is certainly abelian.

**Chapter 3.1 Exercise 9:** Define  $\phi : \mathbb{C}^\times \rightarrow \mathbb{R}^\times$  by  $\phi(a + bi) = a^2 + b^2$ . Prove that  $\phi$  is a homomorphism and find the image of  $\phi$ . Describe the kernel and the fibers of  $\phi$  geometrically as subsets of the plane.

**Solution:** Let  $x = a + bi$  and  $y = c + di$  be two elements of  $\mathbb{C}^\times$ . Then

$x \cdot y = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$ . So,

$$\begin{aligned}
 \phi(x \cdot y) &= \phi((ac - bd) + (ad + bc)i) \\
 &:= (ac - bd)^2 + (ad + bc)^2 \\
 &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\
 &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\
 &= a^2(c^2 + d^2) + b^2(c^2 + d^2) \\
 &= (a^2 + b^2)(c^2 + d^2) := \phi(x)\phi(y).
 \end{aligned}$$

So  $\phi$  is a group homomorphism. The image of  $\phi$  is  $(0, \infty)$ . As  $a^2 + b^2$  is non-negative, clearly the image of  $\phi$  must lie in  $[0, \infty)$ , but the only way that  $a^2 + b^2 = 0$  is for  $a = b = 0$ .  $0$  is not an element of  $\mathbb{C}^\times$ , so the image of  $\phi$  is a subset of  $(0, \infty)$ . Conversely, given any  $a \in (0, \infty)$ , the complex number  $\sqrt{a} + 0i$  is invertible ( $\frac{1}{\sqrt{a}} + 0i$  is its multiplicative inverse) and hence an element of  $\mathbb{C}^\times$ . Checking that  $\phi(\sqrt{a}) = a$  shows that the image of  $\phi$  is in fact all of  $(0, \infty)$ .

**Chapter 3.1 Exercise 16:** Let  $G$  be a group, let  $N$  be a normal subgroup of  $G$  and let  $\bar{G} = G/N$ . Prove that if  $G = \langle x, y \rangle$  then  $\bar{G} = \langle \bar{x}, \bar{y} \rangle$ . Prove more generally that if  $G = \langle S \rangle$  for any subset  $S$  of  $G$ , then  $\bar{G} = \langle \bar{S} \rangle$ .

**Solution:** The general statement clearly subsumes the original statement, so we'll prove the more general statement. Let  $x$  be a coset element of  $G/N$ , and  $a$  an element in the coset. As  $G = \langle S \rangle$  we may write  $a$  as a product of elements  $t_1 \cdots t_k$  where the  $t_i$  or their inverses are elements of  $S$ . After applying the map  $\bar{\cdot} : G \rightarrow G/N$  we have

$$x := aN = t_1N \cdots t_kN := \bar{t}_1 \cdots \bar{t}_k$$

where the elements  $\bar{t}_i$  or their inverses lie in  $\bar{S}$ . Thus  $\bar{G} = \langle \bar{S} \rangle$ .

**Chapter 3.1 Exercise 22:**

- (a) Prove that if  $H$  and  $K$  are normal subgroups of a group  $G$  then their intersection  $H \cap K$  is also a normal subgroup of  $G$ .
- (b) Prove that the intersection of an arbitrary nonempty collection normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

**Solution:**

- (a) We already know that the intersection of two subgroups of a group  $G$  is

a subgroup. It remains to show that if  $H$  and  $K$  are normal subgroups then  $H \cap K$  is normal as well. To that end, let  $g$  be an element of  $G$ . Since  $H \cap K$  is a subset of  $H$  and  $H$  is normal, we must have that  $g(H \cap K)g^{-1} \subset H$ . By the same logic we also have  $g(H \cap K)g^{-1} \subset K$ .

Now the map  $x \mapsto gxg^{-1}$  is one-to-one so when  $H \cap K$  is finite, this implies that  $g(H \cap K)g^{-1} = H \cap K$ . When  $H \cap K$  is infinite we have to say a little more. We have shown that for any  $g \in G$  there is an injective map  $\Phi_g : H \cap K \rightarrow H \cap K$  which is given by conjugating elements with  $g$ . We need to show it is onto. Notice though that since we are free to pick whatever  $g$  we like, we can consider  $\Phi_{g^{-1}}$ . Now we check that for any  $x \in G$  we have  $\Phi_g \circ \Phi_{g^{-1}}(x) = \Phi_g(g^{-1}x(g^{-1})^{-1}) = \Phi_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = (gg^{-1})x(gg^{-1}) = x$ . And so  $\Phi_g \circ \Phi_{g^{-1}}$  is the identity map, which is onto. This implies that  $\Phi_g$  must be onto.

(b) OK, the bit about countable collections is a little out of the way probably for some of you, but to give you a very simple taste: the real line  $\mathbb{R}$  is a group under addition. Any element  $r \in \mathbb{R}$  generates a subgroup  $\langle r \rangle$  isomorphic to  $\mathbb{Z}$ . Notice that there are as many of these subgroups as there are elements in  $(0, \infty)$ . Some of you may have learned in another math class that the number of elements in the set  $(0, \infty)$  is quantitatively larger than the number of elements in  $\mathbb{N}$  (and in turn there many other sets with cardinalities larger than  $(0, \infty)$ ). In other words, you cannot list all the subgroups using a standard list  $N_1, N_2, \dots$ . Such a list would have cardinality equal to  $\mathbb{N}$ , and we need to effectively list all the numbers in  $(0, \infty)$  which according to my claim is strictly larger than  $\mathbb{N}$  (strictly larger means there are no set bijections between  $\mathbb{N}$  and  $\mathbb{R}$ ..only injections). Now what the book DOESN'T want you to do is say then, "suppose we have some normal subgroups  $N_1, N_2, \dots$  then we will show that  $\bigcap_{i=0}^{\infty} N_i$  is a blah, blah, blah". This is because your proof would only cover situations where you have a countable, or enumerable number of subgroups. It would not cover the situation I sketched above where you cannot enumerate the subgroups using natural numbers. (PS - I know very little about this stuff, but some mathematicians devote their whole lives to constructing and studying humongous sets that are waaaaaay bigger than  $\mathbb{R}$ .)

OK, so what the book DOES want you to say is something like this: Suppose we have a collection of normal subgroups  $\{N_\alpha\}_{\alpha \in I}$  where  $I$  is some indexing set. This is mathspeak for saying, "start with a bijection from

our collection of normal subgroups to some set  $I$  (which may have a huge cardinality for all we know, or hey, it might be a set with one element)". For instance, in the example I gave you, a good choice for an indexing set  $I$  for all cyclic subgroups generated by an element of  $\mathbb{R}$  would be  $I := (0, \infty)$ . Okay, now lets do the proof, which you will see is basically a fancier looking version of (a).

Suppose we have a collection of normal subgroups  $\{N_\alpha\}_{\alpha \in I}$  where  $I$  is some indexing set. Let  $g$  be an element of  $G$  and  $\alpha$  an element of  $I$ . Since  $\bigcap_{\alpha \in I} N_\alpha$  is a subset of  $N_\alpha$  and  $N_\alpha$  is normal, we must have that  $g(\bigcap_{\alpha \in I} N_\alpha)g^{-1} \subset N_\alpha$ . As this is true for each  $\alpha \in I$  we have  $g(\bigcap_{\alpha \in I} N_\alpha)g^{-1} \subset \bigcap_{\alpha \in I} N_\alpha$ . We have shown that for any  $g \in G$  there is an injective map  $\Phi_g : \bigcap_{\alpha \in I} N_\alpha \rightarrow \bigcap_{\alpha \in I} N_\alpha$  which is given by conjugating elements with  $g$ . We need to show it is onto. Notice though that since we are free to pick whatever  $g$  we like, we can consider  $\Phi_{g^{-1}}$ . Now we check that for any  $x \in G$  we have  $\Phi_g \circ \Phi_{g^{-1}}(x) = \Phi_g(g^{-1}x(g^{-1})^{-1}) = \Phi_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = (gg^{-1})x(gg^{-1}) = x$  And so  $\Phi_g \circ \Phi_{g^{-1}}$  is the identity map, which is onto. This implies that  $\Phi_g$  must be onto.

**Chapter 3.1 Exercise 31:** Prove that if  $H \leq G$  and  $N$  is a normal subgroup of  $H$  then  $H \leq N_G(N)$ . Deduce that  $N_G(N)$  is the largest subgroup of  $G$  in which  $N$  is normal.

**Solution:** By definition,  $N_G(N)$  is the set of elements  $g \in G$  for which conjugation by  $g$  maps  $N$  to itself bijectively. We already know that  $N_G(N)$  is a subgroup of  $G$ . If  $N \triangleleft H$ , then every  $h \in H$  maps  $N$  bijectively to itself under conjugation by  $h$ , and hence  $H \leq N_G(N)$ .

Consider the collection,  $\mathcal{S}$  of subgroups of  $G$  in which  $N$  is normal.  $N_G(N)$  is a subgroup of  $G$  and by its definition,  $N$  is a normal subgroup of  $N_G(N)$ . Thus  $N_G(N)$  is an element in  $\mathcal{S}$ . The first part of this exercise shows that any other element  $H \in \mathcal{S}$  is a subgroup of  $N_G(N)$ . Hence we can say  $N_G(N)$  is the largest subgroup of  $G$  in which  $N$  is normal. Um...this problem just amounts to word play...

**Chapter 3.1 Exercise 36:** Prove that if  $G/Z(G)$  is cyclic then  $G$  is abelian.

**Solution:** As an aside, notice that if this exercise is true, then as  $G$  is

abelian,  $Z(G) = G$ , so  $G/Z(G)$  is the trivial group. So this exercise shows that if  $G/Z(G)$  is cyclic, then it must be trivial....now for the proof.

Suppose that  $x \in G/Z(G)$  is a generator and let  $g$  be an element  $G$ .  $g$  lies in the coset  $gZ(G)$  which is equal to the coset  $x^a Z(G)$  for some  $a \in \mathbb{Z}$  since by hypothesis  $x$  is a generator for  $G/Z(G)$ . But  $gZ(G) = x^a Z(G)$  implies that there exists some  $z \in Z(G)$  such that  $g = x^a z$ . In summary, any element of  $G$  is equal to the product  $x^a z$  for some  $a \in \mathbb{Z}$  and  $z \in Z(G)$ .

Now suppose we have been granted two elements  $g_1$  and  $g_2$  in  $G$ . By our previous work we know that  $g_1 = x^{a_1} z_1$  and  $g_2 = x^{a_2} z_2$  for  $a_1, a_2 \in \mathbb{Z}$  and  $z_1, z_2 \in Z(G)$ . Then we have

$$g_1 g_2 = (x^{a_1} z_1)(x^{a_2} z_2) = x^{a_1} (z_1 x^{a_2}) z_2$$

and since  $z_1 \in Z(G)$  it commutes with all elements of  $G$  so the above expression equals

$$= (x^{a_1} x^{a_2})(z_1 z_2) = x^{a_2} x^{a_1} z_1 z_2$$

and now since  $z_2 \in Z(G)$  we may commute it past  $z_1$  and  $x^{a_1}$  to obtain

$$= x^{a_2} z_2 x^{a_1} z_1 = g_2 g_1.$$

**Chapter 3.3 Exercise 2:** Prove all parts of the lattice isomorphism theorem: Let  $G$  be a group and let  $N$  be a normal subgroup of  $G$ . Then there is a bijection from the set of subgroups  $A$  of  $G$  which contain  $N$  onto the set of subgroups  $\bar{A} = A/N$  of  $G/N$ . In particular, every subgroup of  $\bar{G}$  is of the form  $A/N$  for some subgroup  $A$  of  $G$  containing  $N$  (namely, its preimage in  $G$  under the natural projection homomorphism from  $G$  to  $G/N$ ). This bijection has the following properties: for all  $A, B \leq G$  with  $N \leq A$  and  $N \leq B$ ,

- (1)  $A \leq B$  if and only if  $\bar{A} \leq \bar{B}$ ,
- (2) if  $A \leq B$ , then  $|B : A| = |\bar{B} : \bar{A}|$ ,
- (3)  $\langle A, B \rangle = \langle \bar{A}, \bar{B} \rangle$ ,
- (4)  $\overline{A \cap B} = \bar{A} \cap \bar{B}$ , and
- (5)  $A \triangleleft G$  if and only if  $\bar{A} \triangleleft \bar{G}$ .

**Solution:** Warning: this is an important exercise, and it is an abstract exercise, and it is a long exercise and it is a tedious exercise. It is easy to get

bored writing or reading the solution to this problem, and it may seem a bit pedantic, but do try to follow what's going on.

Before solving the problem, let's check the map  $A \mapsto \bar{A} = A/N$  is well-defined i.e.  $A/N$  makes sense and it is a subgroup of  $G/N$ . Because  $N$  is normal in  $G$ ,  $N$  is normal in any subgroup of  $G$  which contains it. Thus the cosets  $A/N$  form a group.

Now for any group of the form  $A/N$  there is a natural injective group homomorphism into  $G/N$  which allows us to consider  $A/N$  as a subgroup of  $G/N$ . It is defined by sending the coset  $aN$  (as a coset of  $N$  in  $A$ ) to the coset  $aN$  (as a coset of  $N$  in  $G$ ). This map is well defined. Indeed, if we take two different elements  $a$  and  $b$  that represent the same coset of  $N$  in  $A$  then we have  $a^{-1}b \in N$ . But  $a^{-1}b \in N$  implies that  $a$  and  $b$  represent the same coset of  $N$  in  $G$  as well. It is easy to see this map is a group homomorphism. Lastly we note it is injective. For suppose  $aN$  and  $bN$  are two cosets of  $N$  in  $A$  for which  $aN = bN$  as cosets in  $G$ . Then we have  $a^{-1}b \in N$ . But this implies that  $aN = bN$  as cosets of  $N$  in  $A$  as well. Thus we have confirmed that  $A \mapsto A/N$  is a map from the set of subgroups of  $G$  containing  $N$  to the set of subgroups of  $G/N$ .

We verify this map is a bijection, but first we make some preliminary, basic remarks that are somehow confusing anyway. Recall that the coset  $aN$  is the set  $\{an \mid n \in N\}$  and  $aN \in A/N$  is equivalent to saying  $\{an \mid n \in N\} \subset A$ . Since  $1 \in N$ , we have  $a \in \{an \mid n \in N\}$ , so in particular we have  $aN \in A/N$  implies  $a \in A$ . To show our map is injective, suppose that  $A$  and  $B$  are two subgroups of  $G$  which contain  $N$  and suppose that  $A/N = B/N$ . Let  $a$  be an element of  $A$ . We have that the coset  $aN \in A/N = B/N$ , so  $aN \in B/N$  which implies that  $a \in B$  by earlier remarks. Thus  $A \subset B$ . A symmetric argument shows that  $B \subset A$  hence  $A = B$  and the injectivity of the map is shown. To show surjectivity, let  $C$  be a subgroup of  $G/N$ . Then define

$$\hat{C} := \{g \in G \mid gN \in C\}.$$

The set  $\hat{C}$  is actually a subgroup of  $G$ . For let  $a$  and  $b$  be elements of  $\hat{C}$ . Then  $aN$  and  $bN$  are elements of  $C$ . And because  $C$  is a group,  $aNbN$  is an element of  $C$  as well. But  $aNbN = abN$  which shows that  $ab$  is an element of  $\hat{C}$ . Also because  $C$  is a group, it must contain  $(aN)^{-1}$ . As  $(aN)^{-1} = a^{-1}N$  we conclude that  $a^{-1} \in \hat{C}$ . Thus  $\hat{C}$  is a subgroup of  $G$ . It is clear from the definition of  $\hat{C}$  that  $\hat{C}/N = C$ .

Now we can verify (1)-(5)

(1) Suppose  $A \subset B$ . Let  $aN = \{an \mid n \in N\}$  be a coset in  $A$ . Since  $A \subset B$ ,  $a \in B$ , so  $\{an \mid n \in N\} \subset B$  hence  $aN \in B/N$ . So  $A/N \leq B/N$ . Conversely suppose  $A/N \leq B/N$ . Let  $a \in A$ . Then the coset  $aN$  is an element of  $A/N$  and then by our assumption, an element of  $B/N$ . Recall though that this implies that  $B$  contains all the elements in the coset  $aN$  which includes in particular the element  $a$ . So  $A \subset B$ .

(2) We define a map on the coset of  $A$  in  $B$  to the cosets of  $A/N$  in  $B/N$  by the rule

$$rA \mapsto \bar{r}A/N$$

where  $\bar{r}$  stands for the coset element  $rN \in B/N$ . We should check this map is well-defined (it doesn't depend on which coset representative we pick). The set  $\bar{r}A/N$  stands for the set  $\{raN \mid aN \text{ is a left coset of } N \text{ in } A\}$ . Now suppose  $s$  and  $r$  are two elements in  $B$  that represent the same left coset of  $A$  in  $B$ , ie.  $r^{-1}s \in A$ . Suppose  $L$  is a coset in the set  $\bar{r}A/N$ , so  $L = raN$  for some  $a \in A$ . We claim that  $L = sa'N$  for some other  $a' \in A$  and hence is in the set  $\bar{s}A/N$ . Indeed  $L = raN = r(r^{-1}s)(r^{-1}s)^{-1}aN = (rr^{-1})s(r^{-1}s)^{-1}aN = s(r^{-1}s)^{-1}aN$ . Since  $r^{-1}s \in A$ , the element  $a' := (r^{-1}s)^{-1}a \in A$ . Hence we conclude  $L = sa'N$ , and so  $L \in \bar{s}A/N$ . Thus  $\bar{r}A/N \subset \bar{s}A/N$  and by a symmetric argument we have  $\bar{s}A/N \subset \bar{r}A/N$  and so they are in fact equal. Thus our map is well-defined.

We claim the map is a bijection, thus verifying (2). It is injective. For if  $\bar{r}A/N = \bar{s}A/N$  then there are left cosets  $aN$  and  $a'N$  of  $N$  in  $A$  such that the left coset  $raN$  is equal to  $sa'N$ . But this implies that  $(ra)^{-1}(sa') = a^{-1}r^{-1}sa'$  is an element of  $N$  and hence also an element of  $A$ . Multiplying our expression by  $a$  on the left and  $a'^{-1}$  on the right shows that  $r^{-1}s$  is an element of  $A$  and hence  $rA = sA$ . As for surjectivity, suppose we have a left coset  $L$  of  $A/N$  in  $B/N$ . Pick a representing element of  $L$ , which is a coset of  $N$  in  $B$ , represented say by the element  $x \in B$ . Then it is clear that the coset  $xA$  maps to  $L$ .

(3) The subgroup  $A$  is a subgroup of  $\langle A, B \rangle$ . By (1) we have  $\bar{A} \leq \overline{\langle A, B \rangle}$ . By similar reasoning we have  $\bar{B} \leq \overline{\langle A, B \rangle}$ . Now by definition,  $\langle \bar{A}, \bar{B} \rangle$  is the smallest subgroup of  $G/N$  which contains  $\bar{A}$  and  $\bar{B}$ . Since  $\overline{\langle A, B \rangle}$  contains  $\bar{A}$  and  $\bar{B}$  we must have

$$\langle \bar{A}, \bar{B} \rangle \leq \overline{\langle A, B \rangle}.$$

It remains to show the opposite inclusion. To that end, recall that we've shown the map  $A \rightarrow \overline{A}$  surjects onto the set of subgroups of  $G/N$ . Then as  $\langle \overline{A}, \overline{B} \rangle$  is a subgroup of  $G/N$  we may let  $C$  be a subgroup of  $G$  such that  $\overline{C} = \langle \overline{A}, \overline{B} \rangle$ . Notice that as  $\overline{A} \leq \langle \overline{A}, \overline{B} \rangle$  we may use (1) to conclude that  $A \leq C$ . Similarly we reason that  $B \leq C$ . Since  $\langle A, B \rangle$  is contained in all subgroups of  $G$  which contain both  $A$  and  $B$ , it must be the case that  $\langle A, B \rangle \leq C$ . Using (1) one more time we conclude

$$\overline{\langle A, B \rangle} \leq \overline{C} := \langle \overline{A}, \overline{B} \rangle.$$

(4) As  $A \cap B \leq A$  we know from (1) that  $\overline{A \cap B} \leq \overline{A}$ . Similarly we have  $\overline{A \cap B} \leq \overline{B}$ . Hence  $\overline{A \cap B} \leq \overline{A} \cap \overline{B}$ . Now suppose we have  $x \in \overline{A} \cap \overline{B} := A/N \cap B/N$ . Then the coset  $x$  is a subset of  $A$  and a subset of  $B$ , so it is a subset of  $A \cap B$ . Hence  $x \in \overline{A \cap B}$  and  $\overline{A \cap B} \leq \overline{A} \cap \overline{B}$ .

(5) Suppose that  $\overline{A} \triangleleft \overline{G}$  and  $g$  is any element of  $G$ . As the map  $G \rightarrow G/N$  is a group homomorphism,  $\overline{gAg^{-1}} = \overline{g} \overline{A} \overline{g}^{-1}$  and since  $\overline{A}$  is normal, we have  $\overline{g} \overline{A} \overline{g}^{-1} = \overline{A}$ , and so

$$\overline{gAg^{-1}} = \overline{A}.$$

From the first portion of this exercise we verified the map  $A \mapsto \overline{A}$  is an injective map, hence we conclude that  $gAg^{-1} = A$ .

Now suppose that  $A$  is normal in  $G$  and let  $\overline{g}$  be an element of  $G/N$ . Also let  $g \in \overline{g}$  be an element in this coset. Now  $\overline{gAg^{-1}} = \overline{g} \overline{A} \overline{g}^{-1}$  and as  $A$  is normal in  $G$ ,  $gAg^{-1} = A$ . Thus

$$\overline{A} = \overline{g} \overline{A} \overline{g}^{-1},$$

which was to be shown.

**Chapter 3.3 Exercise 3:** Prove that if  $H$  is a normal subgroup of  $G$  of prime index  $p$  then for all  $K \leq G$  either

- (i)  $K \leq H$  or
- (ii)  $G = HK$  and  $|K : K \cap H| = p$ .

**Solution:** As  $H$  is a normal subgroup of  $G$  and  $K$  is a subgroup of  $G$  we can use the second isomorphism theorem which states that  $HK$  is a subgroup of

$G$ ,  $H$  is a normal subgroup of  $HK$ ,  $H \cap K$  is a normal subgroup of  $K$ , and that

$$HK/H \cong K/H \cap K.$$

In particular we have  $H \triangleleft HK \triangleleft G$  which implies, from a previous HW's exercise, that  $p = [G : H] = [G : HK][HK : H]$ . As  $p$  is prime we must have that either  $[G : HK] = 1$  or  $[HK : H] = 1$ . If  $[G : HK] = 1$  then  $G = HK$ . The second isomorphism theorem now states that  $G/H \cong K/H \cap K$ . If we forget the group structure, then the equation becomes  $[G : H] = [K : H \cap K]$  as a bijection of sets. Thus  $[G : HK]$  implies the conditions in (ii). Now suppose that  $[HK : H] = 1$ , or in other words that  $HK = H$ . Then the group  $HK/H$  is the trivial group, so by the second isomorphism theorem, we must have that  $K/H \cap K$  is trivial too. This is equivalent to  $K = H \cap K$  which in turn is equivalent to  $K \leq H$ .

**Chapter 3.3 Exercise 9:** Let  $p$  be a prime and let  $G$  be a group of order  $p^a m$ , where  $p$  does not divide  $m$ . Assume  $P$  is a subgroup of  $G$  of order  $p^a$  and  $N$  is a normal subgroup of  $G$  of order  $p^b n$  where  $p$  does not divide  $n$ . Prove that  $|P \cap N| = p^b$  and  $|PN/N| = p^{a-b}$ . (This exercise shows that the intersection of any Sylow  $p$ -subgroup of  $G$  with normal subgroup  $N$  is a Sylow  $p$ -subgroup of  $N$ .)

**Solution:** By Lagrange's theorem, since  $N$  is a subgroup of  $G$  we must have  $p^b n | p^a m$  and in particular that  $b \leq a$ . Also since  $P \cap N$  is a subgroup of  $N$  and of  $P$  it must be the case that  $|P \cap N|$  divides  $p^b n$  and  $p^a$ . Thus  $|P \cap N| = p^c$  from some  $c \leq \min(a, b) = b$ . Finally since  $PN$  is a subgroup of  $G$ ,  $|PN|$  divides  $p^a n$  so  $|PN| = p^d r$  for some  $d \leq a$  and some  $r$  relatively prime to  $p$ . Now, the second isomorphism theorem tells us that

$$PN/N \cong P/N \cap P.$$

A group isomorphism is in particular an isomorphism of sets (a bijection) so we conclude that

$$|PN/N| = |P/N \cap P|.$$

As  $G$  is a finite group, we know that  $|PN/N| = \frac{|PN|}{|N|}$  and  $|P/N \cap P| = \frac{|P|}{|N \cap P|}$ . Hence

$$\frac{|PN|}{|N|} = \frac{|P|}{|N \cap P|}$$

$$|PN||N \cap P| = |P||N|.$$

$$p^d r p^c = p^a p^b n.$$

From this we conclude that  $r = n$  and  $d + c = a + b$ . Along with the inequalities  $d \leq a$  and  $c \leq b$ , the equation  $d + c = a + b$  implies that  $d = a$  and  $b = c$ . Thus  $|N \cap P| = p^b$  and  $|PN/N| = \frac{|PN|}{|N|} = \frac{p^a n}{p^b n} = p^{a-b}$ .

**Chapter 3.4 Exercise 1:** Prove that if  $G$  is an abelian simple group then  $G \cong \mathbb{Z}/p$  for some prime  $p$  (do not assume that  $G$  is finite).

**Solution:** If  $G$  is abelian, then the condition of being simple is equivalent to requiring that  $G$  has no subgroups besides  $G$  itself and the trivial subgroup because all subgroups of an abelian group are normal. First suppose  $G$  is an infinite abelian simple group. Let  $x$  be a non-trivial element of  $G$ , and consider the subgroup generated by  $x$ . Since  $x$  is non-trivial,  $\langle x \rangle$  must be equal to  $G$  instead (as  $G$  cannot have any proper non-trivial subgroups). But  $\langle x \rangle$  is isomorphic to  $\mathbb{Z}$ . This is a problem because we now have  $G \cong \mathbb{Z}$  and  $\mathbb{Z}$  is not exactly simple. For instance  $2\mathbb{Z}$  is a non-trivial proper subgroup of  $\mathbb{Z}$ . Thus there can be no infinite abelian simple groups.

Now suppose that  $G$  is a finite abelian simple group. As before let  $x$  be a non-trivial element of  $G$ . Then as before, we must have  $\langle x \rangle = G$ . This implies that  $G \cong \mathbb{Z}/n$  for some  $n \in \mathbb{N}$ . If  $n$  is not prime, then we claim that  $\mathbb{Z}/n$  is not simple. For if  $n$  is composite,  $n = dr$  for some natural numbers  $d, r > 1$ . Consider the element  $x^r$ . It has order  $d$ , and we see that the subgroup it generates also has order  $d$  which is strictly less than  $n$  and greater than 1. This is a proper non-trivial subgroup of  $G$ , so  $G$  is not simple.

Lastly we show that  $\mathbb{Z}/p$  is simple when  $p$  is prime. By Lagrange's theorem, if  $N$  is a subgroup of  $\mathbb{Z}/p$  by Lagrange's theorem we have  $|N|$  divides  $p$ . As  $p$  is prime we must have  $|N| = 1$  or  $|N| = p$ . In the first case,  $N$  must be the trivial subgroup. In the latter case, we see that  $N$  must be all of  $\mathbb{Z}/p$ . Evidently  $\mathbb{Z}/p$  can have no non-trivial proper subgroups. Hence it is simple.

**Chapter 3.5 Exercise 2:** Prove that  $\sigma^2$  is an even permutation for every permutation  $\sigma$ .

**Solution:** Recall that the sign of a permutation  $\sigma$  is determined by a group homomorphism  $\epsilon : S_n \rightarrow \{+1, -1\} \cong \mathbb{Z}/2$ . The even permutations are those elements that are in the kernel of  $\epsilon$  and the odd permutations are all the other elements. Now  $\epsilon(\sigma^2) = (\epsilon(\sigma))^2$  because  $\epsilon$  is a group homomorphism. Also  $(\epsilon(\sigma))^2 = 1$  because all two of the elements of  $\mathbb{Z}/2$  have order dividing

2. Thus we conclude that  $\epsilon(\sigma^2) = 1$  which means that  $\sigma^2$  is an even permutation.

**Chapter 3.5 Exercise 4:** Show that  $S_n = \langle (12), (123 \cdots n) \rangle$ .

**Solution:** The set of all transpositions generate  $S_n$ , hence it suffices to show that all transpositions lie in  $\langle (12), (123 \cdots n) \rangle$ . First we check that for  $1 \leq i \leq n$  the following formula holds:

$$(i \ i + 1) = (12 \cdots n)^{i-1} (12) (12 \cdots n)^{1-i}$$

(where in the case when  $i = n$ ,  $(i \ i + 1)$  should be replaced with  $(n \ 1)$ ). This shows that all transpositions must lie in  $\langle (12), (123 \cdots n) \rangle$  as they are products of elements of  $\langle (12), (123 \cdots n) \rangle$ . Now also note that for any  $2 \leq a \leq n$  the following formula holds:

$$(1a) = (12)(23) \cdots (a-2 \ a-1)(a-1 \ a)(a-2 \ a-1) \cdots (23)(12).$$

This shows that any transposition  $(1a)$  can be written as a product of transpositions of the form  $(i \ i + 1)$  which we already showed were elements of  $\langle (12), (123 \cdots n) \rangle$ . Thus all transpositions of the form  $(1a)$  are elements of  $\langle (12), (123 \cdots n) \rangle$ . But finally note that for any  $1 \leq a \neq b \leq n$  we have

$$(ab) = (1a)(1b)(1a).$$

So by the same logic as before, since  $(ab)$  has been written as a product of elements in  $\langle (12), (123 \cdots n) \rangle$ ,  $(ab)$  must be an element of  $\langle (12), (123 \cdots n) \rangle$ . This is what we needed to show.

**Chapter 3.5 Exercise 12:** Prove that  $A_n$  contains a subgroup isomorphic to  $S_{n-2}$  for each  $n \geq 3$ .

**Solution:** Identify  $S_{n-2}$  as the group of permutations on the set  $\{3, 4, \dots, n\}$ . Define the map  $\phi$  by

$$\begin{aligned} \phi : S_{n-2} &\longrightarrow S_n \\ \sigma &\mapsto \begin{cases} \sigma & \text{if } \sigma \text{ is even} \\ \sigma(12) & \text{if } \sigma \text{ is odd} \end{cases} \end{aligned}$$

We make the following claims:

- 1)  $\phi$  is a homomorphism,
- 2)  $\phi$  is one-to-one,

3) The image of  $\phi$  is a subgroup of  $A_n$ .

Together, these three claims prove Exercise 12. Indeed,  $S_{n-2}$  is isomorphic to  $\phi(S_{n-2})$  by (1) and (2), and  $\phi(S_{n-2})$  is a subgroup of  $A_n$  by (3).

(1) - Let  $\tau$  and  $\sigma$  be elements of  $S_{n-2}$ . There are four cases to consider, depending on whether  $\tau$  and  $\sigma$  are even or odd. If both are even, then  $\phi(\sigma\tau) := \sigma\tau = \phi(\sigma)\phi(\tau)$ . If  $\sigma$  is odd and  $\tau$  is even then  $\sigma\tau$  is odd. Thus  $\phi(\sigma\tau) = (1\ 2)\sigma\tau = \phi(\sigma)\phi(\tau)$ . Now suppose that  $\sigma$  is even and  $\tau$  is odd.  $\phi(\sigma\tau) := (1\ 2)\sigma\tau$  Now  $\sigma$  and  $\tau$  fix 1 and 2, so they commute with the permutation (1 2) (their cycle decompositions are disjoint to use some lingo), so  $(1\ 2)\sigma\tau = \sigma(1\ 2)\tau = \phi(\sigma)\phi(\tau)$ . The last case is when both  $\sigma$  and  $\tau$  are odd. Then  $\sigma\tau$  is even. So  $\phi(\sigma\tau) := \sigma\tau$  Notice that  $\sigma\tau = (1\ 2)(1\ 2)\sigma\tau$  and again use the fact that (1 2) commutes with  $\sigma$  to conclude  $(1\ 2)(1\ 2)\sigma\tau = (1\ 2)\sigma(1\ 2)\tau : \phi(\sigma)\phi(\tau)$ . Thus  $\phi$  is a group homomorphism.

(2) - Suppose  $\sigma$  is an element of  $S_{n-2}$  and suppose that  $\phi(\sigma) = 1$ . Notice that  $\sigma$  can't be odd. If it were then  $\phi(\sigma) = (1\ 2)\sigma$  and such a permutation clearly swaps 1 and 2. The identity permutation doesn't do this. Now if  $\sigma$  is even, then we have  $1 = \phi(\sigma) = \sigma$ , so  $\sigma$  must be the identity permutation. So the kernel of  $\phi$  is the trivial group. This implies that  $\phi$  is injective.\*\*\*

(3) - The image of  $\phi$  must be a subset of  $A_n$  because if  $\sigma$  is even,  $\phi(\sigma) = \sigma$  is even also. When  $\sigma$  is odd,  $\sigma$  can be written as a product of an odd number of transpositions. But then it is clear that  $\phi(\sigma) = (1\ 2)\sigma$  is a product of an even number of transpositions, hence it is even also.

\*\*\* There is an important and simple fact which maybe you know from class, maybe you don't. It says

“Let  $\phi : G \rightarrow H$  be a group homomorphism. The kernel of  $\phi$  is trivial if and only if  $\phi$  is injective.”

*Proof.*  $\Leftarrow$  If  $\phi$  is injective, then the preimage of any point in  $H$  is either empty or a singleton set. Since  $\phi(1) = 1$ , the preimage of the element 1 is non-empty, so it must be the singleton set containing  $\{1\}$ . Thus the kernel is the trivial group.

$\Rightarrow$  Suppose  $x$  and  $y$  are two elements of  $G$  such that  $\phi(y) = \phi(x)$ . As  $\phi(x)$  is a group element in  $H$  it has an inverse element  $\phi(x)^{-1}$ . Multiply

$\phi(y) = \phi(x)$  on both sides by  $\phi(x)^{-1}$  to get

$$\begin{aligned}\phi(x)^{-1}\phi(y) &= \phi(x)^{-1}\phi(x) \\ \phi(x)^{-1}\phi(y) &= 1 \\ \phi(x^{-1})\phi(y) &= 1 \\ \phi(x^{-1}y) &= 1\end{aligned}$$

From which we see that  $x^{-1}y$  is an element of the kernel of  $\phi$ . By assumption, the kernel consists of only one element, the trivial element, hence  $x^{-1}y = 1$  which implies that  $x = y$ . So  $\phi$  is injective.  $\square$