

# Math 210A

## Homework 4

Brett Hemenway

November 14, 2005

1. Let  $A$  and  $C$  be groups, and  $\theta : C \rightarrow \text{Aut}(A)$  a homomorphism. Let  $A \rtimes_{\theta} C$  be the set  $A \times C$  with a binary operation defined by  $(a, c)(a', c') = (a\theta(c)(a'), cc')$  for  $a, a' \in A$  and  $c, c' \in C$ . This defines a group law because

closed:  $(a, c)(a', c') = (a\theta(c)(a'), cc') \in A \times C$  because  $\theta(c)(a) \in A$ , and  $A$ , and  $C$  are closed.

identity:

$$(a, c)(e_a, e_c) = (a\theta(c)(e_a), ce_c) = (ae_a, c) = (a, c)$$

We have  $\theta(c)(e_a) = e_a$  because  $\theta(c)$  is an automorphism, and

$$(e_a, e_c)(a, c) = (e_a\theta(e_c)(a), e_c c) = (e_a a, c) = (a, c)$$

because  $\theta$  is a homomorphism.

inverse:

$$\begin{aligned}(a, c)(\theta(c^{-1})(a^{-1}), c^{-1}) &= (a\theta(c)(\theta(c^{-1})(a)), cc^{-1}) \\ &= (a\theta(cc^{-1})a^{-1}, cc^{-1}) \\ &= (aa^{-1}, e_c) \\ &= (e_a, e_c)\end{aligned}$$

and

$$\begin{aligned}(\theta(c^{-1})(a^{-1}), c^{-1})(a, c) &= (\theta(c^{-1})(a^{-1})\theta(c^{-1})(a), c^{-1}c) \\ &= (\theta(c^{-1}c)(a^{-1}a), e_c) \\ &= (\theta(e_c)(e_a), e_c) \\ &= (e_a, e_c)\end{aligned}$$

associative:

$$\begin{aligned}
((a_1, c_1)(a_2, c_2))(a_3, c_3) &= (a_1\theta(c_1)(a_2), c_1c_2)(a_3, c_3) \\
&= (a_1\theta(c_1)(a_2)\theta(c_1c_2)(a_3), c_1c_2c_3) \\
&= (a_1\theta(c_1)(a_2)\theta(c_1)(\theta(c_2)a_3), c_1c_2c_3) \\
&= (a_1\theta(c_1)(a_2\theta(c_2)(a_3)), c_1c_2c_3) \\
&= (a_1, c_1)((a_2\theta(c_2)(a_3), c_2c_3)) \\
&= (a_1, c_1)((a_2, c_2)(a_3, c_3))
\end{aligned}$$

So  $A \rtimes_{\theta} C$  is a group.

Suppose  $B \simeq A \rtimes_{\theta} C$ , then let

$$\begin{aligned}
f : A &\rightarrow B \\
a &\mapsto (a, e_c)
\end{aligned}$$

and

$$\begin{aligned}
g : B &\rightarrow C \\
(a, c) &\mapsto c
\end{aligned}$$

$f$  is a homomorphism because

$$f(ab) = (ab, e_c) = (a\theta(e_c)b, e_c e_c) = (a, e_c)(b, e_c) = f(a)f(b)$$

Where the second to last inequality holds because  $\theta$  is a homomorphism.  $f$  is clearly injective because

$$a = b \Leftrightarrow (a, e_c) = (b, e_c)$$

$g$  is clearly a surjective homomorphism, and

$$\ker(g) = \{(a, e_c) : a \in A\} = \text{im}(f) = f(A)$$

So we have the exact sequence

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1 \quad (1)$$

If we define

$$\begin{aligned}
g' : C &\rightarrow B \\
c &\mapsto (e_a, c)
\end{aligned}$$

then  $gg'(c) = g(g'(c)) = g(e_a, c) = c$ , so  $gg^{-1}$  is the identity on  $C$ . For the converse, suppose the sequence (1) is exact, and  $g' : C \rightarrow B$  with  $gg'$  the identity on  $C$ . Let

$$\theta : C \rightarrow \text{Aut}(A)$$

by the rule

$$\begin{aligned} \theta(c) : A &\rightarrow A \\ a &\mapsto f^{-1}(g'(c)f(a)g'(c)^{-1}) \end{aligned}$$

$\theta(c)$  is an automorphism of  $A$  because  $f$  is an isomorphism from  $A$  to  $\text{im}(f)$ , and conjugation by  $g'(c)$  is an automorphism of  $\text{im}(f)$  because  $\text{im}(f) = \ker(g)$  is normal in  $B$ , and finally  $f^{-1}$  is an isomorphism from  $\text{im}(f)$  to  $A$ , then since the composition of three isomorphisms is an isomorphism,  $\theta(c)$  is an isomorphism from  $A \rightarrow A$ .

$\theta$  is a homomorphism because

$$\begin{aligned} \theta(c_1c_2)(a) &= f^{-1}(g'(c_1c_2)f(a)g'(c_1c_2)^{-1}) \\ &= f^{-1}(g'(c_1)g'(c_2)f(a)g'(c_2)^{-1}g'(c_1)^{-1}) \\ &= f^{-1}(g'(c_1)f(f^{-1}(g'(c_2)f(a)g'(c_2)^{-1}))g'(c_1)^{-1}) \\ &= f^{-1}(g'(c_1)f(\theta(c_2)(a))g'(c_1)^{-1}) \\ &= \theta(c_1)(\theta(c_2)(a)) \end{aligned}$$

Now, let

$$\begin{aligned} \phi : A \rtimes_{\theta} C &\rightarrow B \\ (a, c) &\mapsto f(a)g'(c) \end{aligned}$$

We will show that  $\phi$  is an isomorphism.  $\phi$  is a homomorphism because

$$\begin{aligned} \phi((a, c)(a', c')) &= \phi((a\theta(c)a', cc')) \\ &= \phi((af^{-1}(g'(c)f(a')g'(c)^{-1}), cc')) \\ &= f(af^{-1}(g'(c)f(a')g'(c)^{-1}))g'(cc') \\ &= f(a)g'(c)f(a')g'(c)^{-1}g'(c)g'(c') \\ &= (f(a)g'(c))(f(a')g'(c')) \\ &= \phi(a, c)\phi(a', c') \end{aligned}$$

$\phi$  is injective because if  $f(a)g'(c) = f(a')g'(c')$  then

$$\begin{aligned} g'(c) &= f(a)^{-1}f(a')g'(c') \\ &= f(a^{-1}a')g'(c') \end{aligned}$$

which gives

$$g'(c(c')^{-1}) = f(a^{-1}a') \tag{2}$$

but  $\text{im}(f) = \ker(g)$ , so applying  $g$  to both sides gives

$$c(c')^{-1} = e_c$$

so  $c = c'$ . Plugging this back in to equation (2) gives

$$g'(e_c) = e_B = f(a^{-1}a')$$

Since  $f$  is injective, we have that  $a = a'$ .

This shows that  $\phi$  is injective. To show that  $\phi$  is surjective, let  $b \in B$ , with  $g(b) = c$ .  $g$  is an isomorphism from  $B/\ker(g) = B/f(A) \rightarrow C$ , so we have equality of right cosets

$$f(A)b = f(A)g'(c)$$

So  $g'(c)b^{-1} \in f(A)$ . Suppose  $g'(c)b^{-1} = f(a)$ , then  $f(a^{-1})g'(c) = b$ . So  $\phi$  is onto.

2. a. Let  $D_n$  be the dihedral group of order  $2n$ , i.e.  $D_n = \langle \sigma, \tau \rangle$  where  $\sigma^n = e = \tau^2$  and  $\sigma\tau = \tau\sigma^{n-1}$ . Let

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\rightarrow D_n \\ a &\mapsto \sigma^a \end{aligned}$$

Then  $f$  is an injective homomorphism. Let

$$\begin{aligned} g : D_n &\rightarrow \mathbb{Z}/2\mathbb{Z} \\ \sigma^a\tau^c &\mapsto c \end{aligned}$$

Then  $g$  is a surjective homomorphism. Finally, if we let

$$\begin{aligned} g' : \mathbb{Z}/2\mathbb{Z} &\rightarrow D_n \\ c &\mapsto \tau^c \end{aligned}$$

We have that  $gg'$  is the identity on  $\mathbb{Z}/2\mathbb{Z}$ . By problem 1, we have that  $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$  where

$$\begin{aligned}\theta(c)(a) &= f^{-1}(g'(c)f(a)g'(c)^{-1}) \\ &= f^{-1}(\tau^c \sigma^a \tau^c)\end{aligned}$$

So

$$\begin{aligned}\theta(\bar{0})(a) &= f^{-1}(\tau^0 \sigma^a \tau^0) = f^{-1}(\sigma^a) = a \\ \theta(\bar{1})(a) &= f^{-1}(\tau \sigma^a \tau) = f^{-1}(\sigma^{-a}) = -a\end{aligned}$$

- b. Let  $\mathbf{Q}$  the quaternion group of order 8, i.e.  $\mathbf{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$ . If  $\mathbf{Q}$  were the semidirect product of groups, counting gives four possibilities

- (1)  $\mathbf{Q} \simeq \mathbb{Z}/4\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$
- (2)  $\mathbf{Q} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$
- (3)  $\mathbf{Q} \simeq \mathbb{Z}/2\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/4\mathbb{Z}$
- (3)  $\mathbf{Q} \simeq \mathbb{Z}/2\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Case (1) is ruled out because  $\mathbf{Q} \not\cong D_n \simeq \mathbb{Z}/4\mathbb{Z} \rtimes_{\theta} \mathbb{Z}/2\mathbb{Z}$

Case (2) is ruled out because  $\mathbf{Q}$  has only 1 element of order 2 so there is no surjective map  $g$  from  $\mathbf{Q}$  to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

Case (3) is ruled out because if  $f$  injects from  $\mathbb{Z}/2\mathbb{Z}$  to  $\mathbf{Q}$ , then  $f(\mathbb{Z}/2\mathbb{Z}) = \{\pm 1\}$  but then  $\mathbf{Q}/\ker(g) = \mathbf{Q}/\{\pm 1\}$ , but

$$\mathbf{Q}/\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/4\mathbb{Z}$$

Case (4) is ruled out because there is no surjection from  $\mathbf{Q}$  to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  because  $\mathbf{Q}$  has only one element of order 2.

So we conclude that  $\mathbf{Q}$  is not the semidirect product of two non-trivial groups.

3. Let  $H \subset G$  be a subgroup

- a.  $Z_G(H) = \{g \in G : gh = hg \text{ for all } h \in H\}$ . Clearly  $Z_G(H) \subset N_G(H)$ ,  $Z_G(H)$  is normal in  $N_G(H)$  because it is the kernel of the map

$$\begin{aligned}N_G(H) &\rightarrow \text{Aut}(H) \\ g &\mapsto \text{conjugation by } g\end{aligned}$$

- b. The monomorphism from  $N_G(H)/Z_G(H)$  to  $Aut(H)$  was described in part (a).
- c. Let  $G$  be infinite, and  $H$  normal subgroup of  $G$  with  $|H| = n$ . Then from part b we have an injection from  $N_G(H)/Z_G(H) = G/Z_G(H)$  into  $Aut(H) \subset S_n$ . So  $|G/Z_G(H)| \leq n!$ .
4. Let  $G$  be a simple group and  $H$  a subgroup of  $G$  with index  $n < \infty$ . Then  $G$  acts on the cosets  $G/H$ . This gives us a homomorphism from  $G$  to  $S_{G/H} = S_n$ . The kernel of this homomorphism is a normal subgroup of  $G$ , but since  $G$  is simple it must be  $G$  or  $\{e\}$ . It cannot be  $G$  since  $gH \neq H$  for all  $g \in G$ . So the kernel must be trivial. From this we conclude  $G$  injects into  $S_n$ , so  $|G| \leq n!$ .
5. Let  $H \subset G$ .

- a. Suppose  $G$  is solvable, then we have a sequence

$$1 = H_0 \subset H_1 \subset \dots \subset H_n = G$$

with  $H_{i+1}/H_i$  abelian. Consider the sequence

$$1 = H_0 \cap H \subset H_1 \cap H \subset \dots \subset H_n \cap H = H$$

$(H_i \cap H) \triangleleft (H_{i+1} \cap H)$  because  $g(H_i \cap H)g^{-1} \subset H_i$  for  $g \in H_{i+1}$  and  $g(H_i \cap H)g^{-1} \in H$  for  $g \in H$ .

Next, we apply the second isomorphism theorem to the group  $(H \cap H_{i+1})/(H \cap H_i) = (H \cap H_{i+1})/((H \cap H_{i+1}) \cap H_i)$ , this gives

$$(H \cap H_{i+1})/(H \cap H_i) = (H \cap H_{i+1})/((H \cap H_{i+1}) \cap H_i) \simeq H_i(H \cap H_{i+1})/H_i$$

But  $H_i(H \cap H_{i+1})/H_i$  is a subgroup of  $H_{i+1}/H_i$ , so it must be abelian as well. Thus  $H$  is solvable.

- b. Suppose  $H$  and  $G/H$  are solvable. So we have series

$$1 = H'_0 \subset \dots \subset H'_r = G/H$$

with each  $H'_{i+1}/H'_i$  abelian. Then by the correspondence theorem, we have a sequence

$$H = H_0 \subset \dots \subset H_r = G$$

By the third isomorphism theorem  $H_{i+1}/H_i \simeq H'_{i+1}/H'_i$ , so each  $H_{i+1}/H_i$  is abelian. Since  $H$  is solvable, we also have the sequence

$$1 = K_0 \subset \dots \subset K_t = H$$

Splicing these two sequences together we have that  $G$  is solvable because

$$1 = K_0 \subset \dots \subset K_t = H = H_0 \subset \dots \subset H_r = G$$

For the converse, if  $G$  is solvable, by part (a),  $H$  is solvable. Then suppose

$$1 = H_0 \subset \dots \subset H_n = G$$

Consider the series

$$H = HH_0 \subset \dots \subset HH_n = G \quad (3)$$

Each  $HH_i$  is a subgroup of  $G$  because  $H$  is normal in  $G$ .  $HH_i$  is normal in  $HH_{i+1}$  because if  $h \in H$ ,  $h_{i+1} \in H_{i+1}$ , we have

$$\begin{aligned} (hh_{i+1})HH_i(hh_{i+1})^{-1} &= (hh_{i+1})HH_i(h_{i+1}^{-1}h^{-1}) \\ &= H(hh_{i+1})H_i(h_{i+1}^{-1}h^{-1}) \\ &= (Hh)(h_{i+1}H_ih_{i+1}^{-1})h^{-1} \\ &= HH_ih^{-1} \\ &= H_iHh^{-1} \\ &= H_iH \\ &= HH_i \end{aligned}$$

We know each quotient  $H_{i+1}/H_i$  is abelian, and we have surjective homomorphism from  $H_{i+1}/H_i$  to  $HH_{i+1}/HH_i$  given by  $h_{i+1}H_i \mapsto h_{i+1}H_iH = h_{i+1}HH_i$ . So each quotient  $HH_{i+1}/HH_i$  is abelian because  $H_{i+1}/H_i$  is. To see that  $G/H$  is solvable, mod out each term in the series (3) by  $H$ , and apply the third isomorphism theorem.

- c. (i) This is almost identical to the proof of part (a). Suppose  $G$  is polycyclic. Then we have a series

$$1 = H_0 \subset \dots \subset H_n = G$$

with  $H_{i+1}/H_i$  cyclic. Then consider the sequence

$$1 = H_0 \cap H \subset \dots \subset H_n \cap H = H$$

$(H_i \cap H) \triangleleft (H_{i+1} \cap H)$  because  $g(H_i \cap H)g^{-1} \in H_{i+1}$  for  $g \in H_{i+1}$  and  $g(H_i \cap H)g^{-1} \in H$  for  $g \in H$ .

Next, we apply the second isomorphism theorem to the group

$$(H \cap H_{i+1})/(H \cap H_i) = (H \cap H_{i+1})/((H \cap H_{i+1}) \cap H_i)$$

this gives

$$(H \cap H_{i+1})/(H \cap H_i) \simeq H_i(H \cap H_{i+1})/H_i$$

But  $H_i(H \cap H_{i+1})/H_i$  is a subgroup of  $H_{i+1}/H_i$ , since any subgroup of a cyclic group is cyclic, we have that  $(H \cap H_{i+1})/(H \cap H_i)$  is cyclic, thus  $H$  is polycyclic.

(ii) This is almost identical to the proof of part (b).

Suppose  $H$  and  $G/H$  are polycyclic. So we have series

$$1 = H'_0 \subset \dots \subset H'_r = G/H$$

with each  $H'_{i+1}/H'_i$  cyclic. Then by the correspondence theorem, we have a sequence

$$H = H_0 \subset \dots \subset H_r = G$$

By the third isomorphism theorem  $H_{i+1}/H_i \simeq H'_{i+1}/H'_i$ , so each  $H_{i+1}/H_i$  is cyclic. Since  $H$  is polycyclic, we also have the sequence

$$1 = K_0 \subset \dots \subset K_t = H$$

Splicing these two sequences together we have that  $G$  is polycyclic because

$$1 = K_0 \subset \dots \subset K_t = H = H_0 \subset \dots \subset H_r = G$$

For the converse, if  $G$  is polycyclic, by part (c.i),  $H$  is polycyclic. Then suppose

$$1 = H_0 \subset \dots \subset H_n = G$$

Again, consider the series

$$H = HH_0 \subset \dots \subset HH_n = G$$

We have already seen that  $HH_i$  is normal in  $HH_{i+1}$  we know each quotient  $H_{i+1}/H_i$  is cyclic, and we have surjective homomorphism from  $H_{i+1}/H_i$  to  $HH_{i+1}/HH_i$  given by  $h_{i+1}H_i \mapsto h_{i+1}H_iH = h_{i+1}HH_i$ . So each quotient  $HH_{i+1}/HH_i$  is cyclic because  $H_{i+1}/H_i$  is. To see that  $G/H$  is polycyclic, mod out each term in the series by  $H$ , and apply the third isomorphism theorem.

6. A group  $G$  is said to have a composition series if there is a finite chain of subgroups

$$1 \subset H_0 \subset H_1 \subset \dots \subset H_n = G$$

of  $G$  with  $H_i \triangleleft H_{i+1}$  and  $H_{i+1}/H_i$  simple.

- a. The group of order 1 obviously has a composition series  
 Suppose all groups of order less than  $n$  have a composition series  
 Let  $G$  be a group with  $|G| = n$ .  
 If  $G$  is simple, then we have the composition series  $1 \subset G$ .  
 Otherwise let  $H \triangleleft G$ . By our induction assumption  $G/H$  has a composition series

$$1 = H'_0 \subset \dots \subset H'_r \subset G/H$$

with  $H'_{i+1}/H'_i$  simple. Then by the correspondence theorem, we have a sequence of subgroups

$$H = H_0 \subset \dots \subset H_r = G$$

with  $H_{i+1}/H_i$  simple. By our induction assumption,  $H$  has a composition series,

$$1 = K_0 \subset \dots \subset K_t \subset H$$

Then, splicing these two series together we obtain a composition series for  $G$

$$1 = K_0 \subset \dots \subset K_t = H = H_0 \subset \dots \subset H_r = G$$

So any finite group  $G$  has a composition series.

- b. First, note that in any composition series, the first subgroup,  $H_0$  must be simple.  
 Every subgroup of  $\mathbb{Z}$  has the form  $n\mathbb{Z}$ , but  $n\mathbb{Z}$  is not simple because it has a normal subgroup  $2n\mathbb{Z}$ . So  $\mathbb{Z}$  does not have a composition series.
- c. Let  $G$  be a finite solvable group with

$$1 = H_0 \subset \dots \subset H_n = G$$

Each quotient  $H_{i+1}/H_i$  is finite, so by part (a) has a composition series

$$1 = K_0 \subset \dots \subset K_{r_i} = H_{i+1}/H_i$$

with  $K_{j+1}/K_j$  simple. But each  $K_j$  is abelian because  $H_{i+1}/H_i$  is abelian. Each quotient  $K_{j+1}/K_j$  is cyclic, because the only finite abelian simple groups are cyclic, and the correspondence theorem gives us a composition series

$$H_i = \widehat{K}_0 \subset \dots \widehat{K}_{r_i} = H_{i+1}$$

and  $\widehat{K}_{j+1}/\widehat{K}_j \simeq K_{j+1}/K_j$ .

Continuing this process for each neighboring  $H_{i+1}, H_i$ , we can “fill out” our solvable series to make a chain all of whose quotients are abelian and simple, and hence cyclic. So we conclude that any finite solvable group is polycyclic.

- d. We will show that every polycyclic group is finitely generated. Let  $G$  be a polycyclic group with composition series

$$1 = H_0 \subset H_1 \subset \dots \subset H_n = G$$

We proceed by induction on  $n$ .

if  $n = 1$ , then  $G$  is cyclic, so  $G$  is finitely generated.

Assume all groups with a composition series of less than  $n$  terms are finitely generated.

$G/H_{n-1}$  is cyclic, so let  $\langle aH_{n-1} \rangle = G/H_{n-1}$ . Then for any  $g \in G$  there exists an  $k$  such that  $gH_{n-1} = a^kH_{n-1}$ . So  $a^{-k}g = h \in H_{n-1}$ , or  $g = a^k h$  but by our induction assumption  $H_{n-1}$  is finitely generated, so any element in  $G$  can be written as a combination of the generators of  $H_{n-1}$  and  $a$ . So  $G$  is finitely generated.

To show that  $\mathbb{Q}$  is not polycyclic, it remains only to show that  $\mathbb{Q}$  is not finitely generated. This is clear though because the set  $\langle \frac{p_1}{q_1}, \dots, \frac{p_n}{q_n} \rangle$  contains no elements with denominator greater than  $\text{lcm}(q_1, q_2, \dots, q_n)$ , so it cannot be all of  $\mathbb{Q}$ .