UNIVERSITY OF PENNSYLVANIA DEPARTMENT OF MATHEMATICS
Math 370 Algebra Fall Semester 2006
Prof. Gerstenhaber, T.A. Asher Auel

Homework #3 Solutions (due 9/26/06)

Chapter 2 Groups

3.4 a) Let G be a group and $a, b \in G$. Then

$$(aba^{-1})^n = ab^n a^{-1},$$

for all $n \in \mathbb{Z}$.

Proof. For $n = 0$ this is clear since $e = (aba^{-1})^0 = ab^0a^{-1} = aa^{-1}$. For $n > 0$, the idea is that

$$\begin{aligned}(aba^{-1})^n &= (aba^{-1})(aba^{-1})\cdots(aba^{-1})(aba^{-1}) \\ &= ab(aa^{-1})b(aa^{-1})\cdots b(aa^{-1})ba^{-1} \\ &= abb\cdots ba^{-1} = ab^n a^{-1}.\end{aligned}$$

This is enough, but I'll give the formal proof by induction as an example. Suppose $(aba^{-1})^n = ab^n a^{-1}$ holds for some $n > 1$, then note that

$$\begin{aligned}(aba^{-1})^{n+1} &= (aba^{-1})^n(aba^{-1}) \\ &= (ab^n a^{-1})(aba^{-1}) = ab^n(aa^{-1})ba^{-1} = ab^n ba^{-1} \\ &= ab^{n+1}a^{-1},\end{aligned}$$

where we've used the induction hypothesis in the second equality. So by induction, our claimed formula holds for all $n > 0$.

Now we handle the case $n < 0$. For $n = -1$, note that

$$(aba^{-1})(ab^{-1}a^{-1}) = ab(aa^{-1})b^{-1}a^{-1} = a(bb^{-1})a^{-1} = aa^{-1} = e,$$

which shows that $(aba^{-1})^{-1} = ab^{-1}a^{-1}$. Now since, for $n > 0$

$$(aba^{-1})^{-n} = ((aba^{-1})^{-1})^n = (ab^{-1}a^{-1})^n,$$

so applying the case of $n > 0$ to $ab^{-1}a^{-1}$ gives use what we want. □

3.5 Claim: Let $\varphi : G \to G'$ be an isomorphism of groups. Then the inverse mapping $\varphi^{-1} : G' \to G$ is also an isomorphism.

Proof. Since $\varphi : G \to G'$ is an isomorphism, in particular it is a bijection, and so the inverse mapping $\varphi^{-1} : G' \to G$ exists and is also a bijection. So we only need to prove that φ^{-1} is a group homomorphism. To that end, let $a', b' \in G'$. Then since φ is bijective, there exist $a, b \in G$ with $\varphi(a) = a'$ and $\varphi(b) = b'$, i.e. $a = \varphi^{-1}(a')$ and $b = \varphi^{-1}(b')$. Now we have

$$\begin{aligned}\varphi^{-1}(a'b') &= \varphi^{-1}(\varphi(a)\varphi(b)) \\ &= \varphi^{-1}(\varphi(ab)) = ab \\ &= \varphi^{-1}(a')\varphi^{-1}(b'),\end{aligned}$$

where the second equality follows since vp is a homomorphism and the third equality follows from the definition of the inverse mapping. Thus $\varphi^{-1} : G' \to G$ is a homomorphism of groups, and it's bijective by construction, so it's an isomorphism. □

3.12 Claim: Let G be a group and let $\varphi : G \to G$ be the inversion map $\varphi(x) = x^{-1}$ for all $x \in G$. Then

a) φ is a bijection, and

b) $\varphi : G \to G$ is an isomorphism iff G is abelian.

Proof. To a), note that φ is surjective since inverses exist in a group, and φ is injective since inverses are unique.

To b), note that since $\varphi : G \to G$ is a bijection, to prove it's an isomorphism it suffices to show it's a homomorphism. To that end, note that if φ is a homomorphism then for $a, b \in G$ we have

$$ab = (b \in a^{-1})^{-1} = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1})\varphi(a^{-1}) = (b^{-1})^{-1}(a^{-1})^{-1} = ba,$$

so G is abelian. Conversely, if G is abelian, then for all $a, b \in G$ we have

$$\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b),$$

so φ is a homomorphism. □

4.4 Since $\mathbb{Z}$ is an (infinite) cyclic group with generator $1 \in \mathbb{Z}$, any homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$ is determined by a choice of image $\varphi(1) \in \mathbb{Z}$. For $n \in \mathbb{Z}$, let $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ be the homomorphism with $\varphi_n(1) = n$, then for any $a \in \mathbb{Z}$, $\varphi_n(a) = n \cdot a$. Since multiplication of integers distributes over addition, we see that each φ_n is in fact a homomorphism, so the collection $\{\varphi_n : \mathbb{Z} \to \mathbb{Z} \ : \ n \in \mathbb{Z}\}$ constitutes all homomorphisms $\mathbb{Z} \to \mathbb{Z}$. Now we have three cases:

- $\varphi_0 : \mathbb{Z} \to \mathbb{Z}$ is the constant zero map, i.e. the trivial homomorphism. It is neither injective nor surjective.
- $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ for $n \neq 0$ are all injective since

  $$a \in \ker(\varphi_n) \iff na = 0 \iff a = 0,$$

  since we're assuming $n \neq 0$. Thus $\ker(\varphi_n) = \{0\}$, and thus φ is injective.
- $\varphi_1 : \mathbb{Z} \to \mathbb{Z}$ is the identity map, which is an isomorphism and $\varphi_{-1} : \mathbb{Z} \to \mathbb{Z}$ is the "minus" map, which is an isomorphism by 3.12b, since $\mathbb{Z}$ is abelian.
- for $n \neq \pm 1$, $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ is not surjective since for example, $na = 1$ is impossible for $n \neq \pm 1$ and $a \in \mathbb{Z}$, i.e. $1 \in \mathbb{Z}$ is never in the image of any of these maps.

4.17 Claim: Let G be a group and

$$Z(G) = \{c \in G : cg = gc \text{for all} g \in G\} \in G$$

its center. Then $Z(G)$ is a normal subgroup of G.

Proof. We must first show $Z(G)$ is a subgroup. First note that for all $g \in G$, $eg = ge$ by definition so that $e \in Z(G)$. Now for $a, b \in Z(G)$, note that for any $g \in G$, we have

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab),$$

so that again $ab \in Z(G)$. Thus $Z(G)$ is closed under multiplication and contains the identity, so is a subgroup of G.

Finally, for $g \in G$, note that for all $c \in Z(G)$, we have $cg = gc$, i.e. $gcg^{-1} = c \in Z(G)$. Thus the center is a normal subgroup. You could say it's the "most normal" normal subgroup. □

4.22/23 Claim: Let $\varphi : G \to G'$ be a surjective homomorphism of groups. Then

a) If G is cyclic then G' is cyclic.
b) If G is abelian then G' is abelian.
4.23 If $N \subset G$ is a normal subgroup, then $\varphi(N) \subset G'$ is a normal subgroup.

Proof. To a), recall that if G is cyclic with generator $x \in G$, then G can be written (whether G is finite or infinite) as

$$G = < x > = \{x^n : n \in \mathbb{Z}\} = \{\ldots, x^{-2}, x^{-1}, e_G, x, x^2, \ldots\}.$$

Then since vp is surjective,

$$\begin{aligned} G' &= \varphi(G) = \varphi(< x >) \\ &= \{\ldots, \varphi(x^{-2}), \varphi(x^{-1}), \varphi(e_G), \varphi(x), \varphi(x^2), \ldots\} \\ &= \{\ldots, \varphi(x)^{-2}, \varphi(x)^{-1}, e_{G'}, \varphi(x), \varphi(x)^2, \ldots\} \\ &= < \varphi(x) >, \end{aligned}$$

by 3.4a, so G' is cyclic.

To b), for all $a', b' \in G'$, since φ is surjective there exist $a, b \in G$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Then

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a',$$

using the fact that G is abelian in the third equality. Thus G' is abelian.

To 4.23, let $n' \in \varphi(N)$ and $g' \in G'$. First, $\varphi(N) \subset G$ is easily seen to be a subgroup from the fact that $N \subset G$ is a subgroup. We want to now show $\varphi(N) \subset G$ is a normal subgroup.

To that end, we note that as before, since vp is surjective, there exists $g \in G$ such that $\varphi(g) = g'$. Furthermore, note that by 3.6, $\varphi(g^{-1}) = \varphi(g)^{-1} = (g')^{-1}$. By the definition of $\varphi(N)$, there exists $n \in N \subset G$ with $\varphi(n) = n'$. Now since $N \subset G$ is a normal subgroup, we have that $gng^{-1} = m \in N$. Finally, we have that

$$g'n(g')^{-1} = \varphi(g)\varphi(b)\varphi(g^{-1}) = \varphi(gng^{-1}) = \varphi(m) \in \varphi(N),$$

so that as claimed, $vp(N) \subset G$ is a normal subgroup. $\square$