# HW 3 Solutions

April 24, 2009

**Chapter 2.2 Problem 1:** Prove that

$$C_G(A) = \{\ g \mid g^{-1}ag = a \text{ for all } a \in A\ \}.$$

**Solution:** Let us temporarily call the set in question $X$. If $g \in X$, then for any $a \in A$ we have

$$gag^{-1} = g(g^{-1}ag)g^{-1} = (gg^{-1})a(gg^{-1}) = 1a1 = a$$

which shows that $g$ is an element of $C_G(A)$ and hence $X \subset C_G(A)$.

If we take an element $g \in C_G(A)$, similar reasoning shows that for any element $a \in A$, we have

$$g^{-1}ag = g^{-1}(gag^{-1})g = (g^{-1}g)a(g^{-1}g) = 1a1 = a.$$

So by definition, $g$ is an element of $X$ and hence $C_G(A) \subset X$. The two inclusions $X \subset C_G(A)$ and $C_G(A) \subset X$ imply that $C_G(A) = X$.

**Chapter 2.2 Problem 5:** In each of parts (a) through (c) show that for the specified group $G$ and subgroup $A$ of $G$, $C_G(A) = A$ and $N_G(A) = G$.
(a) $G = S_3$ and $A = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$.
(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.
(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

**Solution:**
(a) Recall that conjugation preserves the cycle structure of a permutation. Since $A$ consists of all of the 3-cycles in $S_3$ together with the identity, we see that conjugation by any element of $S_3$ fixes the identity and permutes

the other elements of $A$. Thus every element of $S_3$ is an element of $N_G(A)$. You may check by hand that $(12)(123)(12)^{-1} = (12)(123)(12) = (132)$, so $(12) \notin C_G(A)$. Similarly $(23)(123)(23)^{-1} = (13)(123)(13)^{-1} = (132)$ so they're not elements of $C_G(A)$ either. That leaves the elements of $A$ itself. 1 is always in $C_G(A)$. Also for any element of $g$ of a group, conjugation of $g$ by either $g$ or $g^{-1}$ leaves $g$ fixed ($ggg^{-1} = g$ and $g^{-1}gg = g$). Since (132) is the inverse of (123), conjugating one by the other leaves the element fixed. So both (123) and (132) are elements of $C_G(A)$. By exhaustion we have determined that $C_G(A) = A$.

(b) Notice that our subgroup consists of all elements $s^i r^j$ where $j$ is even. Also note that the effect on the exponent $j$ when conjugated by an element of $D_8$ is to become either $j_1$, $-j_1$, $2j_2 - j_1$, or $j_1 - 2j_2$. In all cases, these are even numbers regardless of the value of $j_2$ provided $j_1$ is even. Thus conjugation of any element in our subgroup by an element of $D_8$ lies in the subgroup. So $N_G(A) = D_8$.

Now suppose we conjugate the element $s$ by an element $s^i r^j$ where $j$ is odd. Depending on whether $i$ is zero or not we obtain $sr^{2j}$ or $sr^{-2j}$. Either way, as $j$ is odd, $2j$ and $-2j$ are not congruent to 0 mod 4, so $s^{2j}$ and $s^{-2j}$ cannot be equal to $s$. Hence all elements of the form $s^i r^j$ with $j$ odd are not in $C_G(A)$. As these elements are precisely the elements in $D_8 - A$, we conclude that $A$ contains $C_G(A)$. On the otherhand, you may check that $s$ and $r^2$ generate the subgroup $A$, and they commute with each other ($sr^2 = r^{-2}s = r^2 s$). Thus the subgroup is commutative, so $A$ is contained in $C_G(A)$.

(c) Conjugating any element $g$ of a group by a power of $g$ leaves $g$ fixed because $(g^i)g(g^i)^{-1} = g^{i+1-i} = g$. Thus any power of $r$ lies in $C_G(A)$ and hence also $N_G(A)$. The remaining elements we must consider are of the form $sr^i$. We check by hand that $s$ in not an element of $C_G(A)$ because $srs^{-1} = r^{-1}ss^{-1} = r^4 \neq r$. This together with the fact that all the powers of $r$ are elements of $C_G(A)$ implies that all elements of the form $sr^i$ cannot be in $C_G(A)$. Indeed, if $sr^i$ were an element of $C_G(A)$, then because $C_G(A)$ is a group and $r^{-i}$ is an element of $C_G(A)$ too, then $sr^i r^{-i}$ would be an element of $C_G(A)$ also. But $sr^i r^{-i}$ is the element $s$ which is not an element of $C_G(A)$. So we conclude that $C_G(A) = A$.

We have yet to determine whether $sr^i$ is an element of $N_G(A)$. To that end, note that for any $j \in \mathbb{Z}$

$$(sr^i)r^j(sr^i)^{-1} = sr^ir^j(r^i)^{-1}s^{-1} = sr^{i+j-i}s^{-1} = sr^js = r^{-j}ss = r^{-j}.$$

As $r^{-j}$ is an element of $A$, we see that elements of the form $sr^i$ lie in $N_G(A)$. We have exhausted all the elements of $G$; each was an element of $N_G(A)$. We conclude that $N_G(A) = G$.

**Chapter 2.2 Problem 6:** Let $H$ be a subgroup of the group $G$.
(a) Show that $H \le N_G(H)$. Give an example to show that this is not necessarily true if $H$ is not a subgroup.
(b) Show that $H \le C_G(H)$ if and only if $H$ is abelian.

**Solution:**
(a) Let $h \in H$. Then $h^{-1} \in H$ because $H$ is closed under inverses. For any element $m \in H$ we then have $hmh^{-1} \in H$ because $H$ is closed under multiplication. This implies that $h$ is an element of $N_G(H)$. Thus $H \le N_G(H)$.

The book is a tiny bit imprecise here. If $H$ is not a subgroup, then it is meaningless to write $H \le N_G(H)$. Probably what they meant was that it is possible to find a subset (not a subgroup) $H$ such that $H$ is not contained in $N_G(H)$. For instance, let $G = S_3$ and let $H = \{(12), (123)\}$. You can check that $(123)^{-1} = (132)$ and that $(123)(12)(132) = (23) \notin H$. Hence $(123) \notin N_G(H)$.

(b) $\Leftarrow$ If $H$ is abelian, and $h \in H$, then $h$ fixes all elements of $H$ by conjugation. For let $m \in H$. Then $hmh^{-1} = hh^{-1}m$ because $H$ is abelian, and $hh^{-1}m = m$.
$\Rightarrow$ Let $m$ and $h$ be elements of $H$. Since $H \le C_G(H)$, we must have that $hmh^{-1} = m$. Multiplying this equation on the right by $h$ yields

$$hmh^{-1}h = mh$$

$$hm = mh.$$

Thus $H$ is abelian.

**Chapter 2.3 Problem 10:** What is the order of $\overline{30}$ in $\mathbb{Z}/54$?

**Solution:** The question is asking us to find the smallest $n \in \mathbb{N}$ such that $30n$ is divisible by 54. That number is precisely $\frac{\text{lcm}(30,54)}{30} = \frac{30 \cdot 54}{\text{gcd}(30,54) \cdot 30} =$

$\frac{54}{\gcd(30,54)} = \frac{54}{6} = 9$. The order is 9.

**Chapter 2.3 Problem 11:** Find all cyclic subgroups of $D_8$. Find a proper subgroup of $D_8$ which is not cyclic.

**Solution:**
As every cyclic group must have a generator, we may find all cyclic subgroups by computing the subgroups of $D_8$ generated by the individual elements of $D_8$. We may end up overcounting though; there may be different elements of $D_8$ that generate the same cyclic subgroup. Here is a list of the elements of $D_8$ and the subgroups they generate:

$$e \qquad \{e\}$$

$$r \qquad \{r, r^2, r^3, e\}$$
$$r^2 \qquad \{r^2, e\}$$
$$r^3 \qquad \{r^3, r^2, r, e\}$$
$$s \qquad \{s, e\}$$
$$sr \qquad \{sr, e\}$$
$$sr^2 \qquad \{sr^2, e\}$$
$$sr^3 \qquad \{sr^3, e\}.$$

Well, that's a lot of subgroups. Looks like $\{e, r, r^2, r^3\}$ appears twice on the list by the way.

For a subgroup that is not cyclic, take $\{e, r^2, s, sr^2\}$.

**Chapter 2.3 Problem 16:** Let $G$ be a group and assume $x$ and $y$ are elements of $G$ with orders $n$ and $m$ respectively. Suppose that $x$ and $y$ commute. Prove that $|xy|$ divides the least common multiple of $m$ and $n$. Need this be true if $x$ and $y$ do not commute? Give an example of commuting elements $x, y$ such that the order of $xy$ is not equal to the lesat common multiple of $|x|$ and $|y|$.

**Solution:** Let $l$ stand for the least common multiple of $n$ and $m$. Then since $x$ and $y$ commute with each other, $(xy)^l$ is equal to $x^l y^l$. By its definition as least common multiple, $l$ is divisible by $n$ and by $m$, so we may say that $l = nd$ and $l = md'$ for two natural numbers $d$ and $d'$. Then we have

$$(xy)^l = x^l y^l = (x^n)^d (y^m)^{d'} = 1^d 1^{d'} = 1.$$

We conclude the proof by showing that for any element $g$ and positive number $n$ such that $g^n = 1$, the order of $g$ divides $n$. As $(sy)^l = 1$, this would show that the order of $xy$ divides the least common multiple of $n$ and $m$. To this end, suppose $g^n = 1$. By the euclidean algorithm, we may write $n = |g|d + r$ where $|g|$ is the order of $g$, $d$ is a non-negative number, and $0 \leq r < |g|$. Then we have

$$1 = g^n = g^{|g|d+r} = (g^{|g|})^d g^r = 1^d g^r = g^r.$$

As $r$ is less than the order of $g$, by definition, the only way that we can have $g^r = 1$ is for $r$ to be zero. This means that $n = |g|d$ i.e. the order of $g$ divides $n$. This concludes the proof.

Of course we should guess the answer is "no" here, given the way they asked the question, and since we used the commutativity of $x$ and $y$ in our proof. Lets look for an example. It'll need to come from a non-commutative group obviously. Take the elements (12) and (23) in $S_3$. Both elements have order 2, so the least common multiple of their orders is two as well. On the otherhand, (12)(23) = (123) and the order of (123) is three. Three does not divide two.

For the last part, take any non-identity element $x$ in your favorite non-trivial group $G$. Let $y$ be equal to $x^{-1}$. Then $x$ and $y = x^{-1}$ commute with one another. As $x$ is not the identity, its order is greater than 1. On the other hand the order of $xy = 1$ is 1.

**Chapter 2.3 Problem 24:** Let $G$ be a finite group and let $x \in G$.
(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.
(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle z \rangle)$.

**Solution:**
(a) As $g$ is an element of $N_G(\langle x \rangle)$, $gxg^{-1}$ must be an element of $\langle x \rangle$. But the elements of $\langle x \rangle$ are of the form $x^a$ where $a \in \mathbb{Z}$.

(b) Suppose that $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$. First we show that conjugating any element $x^k$, $k \in \mathbb{Z}$ by $g$ is also an element of $\langle x \rangle$, in particular it is equal to $x^{ak}$. First we will prove this for non-negative $k$. We proceed inductively noting that the cases $k = 0$ and $k = 1$ are obvious and given respectively. Now assume this is true for $k - 1$, $k > 1$. Then $gx^k g = gx^{k-1}(g^{-1}g)xg = (gx^{k-1}g^{-1})(gxg^{-1}) = x^{a(k-1)}x^a = x^{ak}$. To prove the statement for negative

$k$, note that $(g(x^k)g^{-1})^{-1} = (g^{-1})^{-1}x^{-k}g^{-1} = gx^{-k}g^{-1}$. As $k$ is negative, $-k$ is positive and we can use our previous argument to conclude this is equal to $x^{-ak}$. Thus $(g(x^k)g^{-1})^{-1} = x^{-ak}$. Taking the inverse of both sides yields $gx^kg^{-1} = x^{ak}$.

Since $x^{ak}$ is an element of $\langle x\rangle$ we conclude that $g\ \langle x\rangle\ g^{-1} \subset \langle x\rangle$. Recall that conjugation by an element $g$ is always an injective map. For if $gxg^{-1} = gyg^{-1}$ then after multiplying the equation on the right by $g^{-1}$ and on the left by $g$ we see that $x = y$. At this stage then we see that conjugation by $g$ gives a map from $\langle x\rangle$ to itself that is injective. Since $\langle x\rangle$ is a subgroup of finite group, it must be finite as well. Injective maps from finite sets of the same cardinality must also be surjections and hence bijections. Thus conjugation by $g$ is a bijection from $\langle x\rangle$ to itself. So $g{\in}N_G(\langle z\rangle)$.

**Chapter 2.4 Problem 13:** Prove that the multiplicative group of positive rational numbers is generated by the set $S := \{\ \frac{1}{p} \mid p \text{ is a prime }\}$.

**Solution:** An element in this group is of the form $\frac{a}{b}$ where $a$ and $b$ are natural numbers. Being such, by prime factorization we know that $a = p_1^{\alpha_1}\cdots {p_k}^{\alpha_k}$ and $b = q_1^{\beta_1}\cdots {q_k}^{\beta_l}$ where the $p_i$'s and $q_i'$ are primes. Then $\frac{a}{b} = (\frac{1}{q_1})^{\beta_1}\cdots(\frac{1}{q_l})^{\beta_l}(\frac{1}{p_1})^{-\alpha_1}\cdots(\frac{1}{p_l})^{-\alpha_k}$, which shows that $\frac{a}{b}$ is in the set generated by the elements $\frac{1}{p}$. This shows that the set $S$ generates the multiplicative group of positive rational numbers.

**Chapter 2.4 Problem 15:** Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

**Solution:** Let $p$ be a prime and let $G$ be the subset of $\mathbb{Q}$ consisting of elements of the form $ap^i$ for some integers $a$ and $i$. We verify this is a subgroup of $\mathbb{Q}$. It contain 0. Also if we are given two elements $ap^i$ and $bp^j$ in $G$, then without loss of generality, we may assume $i{\leq}j$, and so $ap^i + bp^j = (a + bp^{j-i})p^i$. $a + bp^{j-i}$ is an integer, so $(a + bp^{j-i})p^i$ is an element of $G$. Lastly, $G$ is clearly closed under inverses.

Now we need to show that $G$ is in fact a proper subgroup of $\mathbb{Q}$. Let $q$ be a prime not equal to $p$. We claim that $\frac{1}{q}{\notin}G$. If it were, we'd have $\frac{1}{q} = ap^i$ for some integers $a$ and $i$. Clearly $i$ cannot be non-negative; if it were $ap^i$ would be an integer, while $\frac{1}{q}$ is not. If $i$ is negative, then we have $p^{-i} = aq$ which implies that the prime $q$ divides some powers of $p$. This violates unique factorization. Hence there is no integer $i$ for which $\frac{1}{q} = ap^i$. Thus $\frac{1}{q} \notin G$ and we conclude that $G$ is a proper subgroup of $\mathbb{Q}$.

Now suppose that $G$ were cyclic. Then it would be generated by an element, say $ap^i$. Then consider the element $ap^{i-1} \in G$. We claim that there is no power of $ap^i$ equal to $ap^{i-1}$. This is because if there were we'd have $nap^i = ap^{i-1}$ for some $n$ (remember $\mathbb{Q}$ is additive, so $x^n$ really means multiply $x$ by $n$). This is a contradiction because if $nap^i = ap^{i-1}$ then after dividing both sides by $ap^{i-1}$ we obtain $np = 1$. As $n$ is an integer and $p$ is a prime number, and hence strictly bigger than 1, this cannot happen.

**Chapter 2.5 Problem 2:** In each of (a) through (d) list all subgroups of $D_{16}$ that satisfy the given condition.
(a) Subgroups that are contained in $\langle sr^2, r^4 \rangle$.
(b) Subgroups that are contained in $\langle sr^7, r^4 \rangle$.
(c) Subgroups that contain $\langle r^4 \rangle$.
(d) Subgroups that contain $\langle s \rangle$.

**Solution:**
(a) The elements $sr^2$ and $r^4$ both have order two and commute with each other. This implies that $\langle sr^2, r^4 \rangle$ is isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ has three non-trivial subgroups, one for each non-identity element of the group. Each subgroup is isomorphic to $\mathbb{Z}/2$. This means that $\langle sr^2, r^4 \rangle$ has three non-trivial subgroups isomorphic to $\mathbb{Z}/2$. They are $\langle sr^2 \rangle$, $\langle r^4 \rangle$, and $\langle sr^2 r^4 \rangle = \langle sr^6 \rangle$.
(b) Identical argument as in (a). In this instance we conclude that $\langle sr^7, r^4 \rangle$ has three non-trivial subgroups isomorphic to $\mathbb{Z}/2$. They are $\langle sr^7 \rangle$, $\langle r^4 \rangle$, and $\langle sr^7 r^4 \rangle = \langle sr^3 \rangle$.
(c) For reasons of time and space we'll just give the answer here. For the general approach, see part (d). The proper subgroups of $D_{16}$ that contain $\langle r^4 \rangle$ are $\langle sr^2, r^4 \rangle$, $\langle s, r^4 \rangle$, $\langle r^2 \rangle$, $\langle sr^3, r^4 \rangle$, $\langle sr^5, r^4 \rangle$, $\langle s, r^2 \rangle$, $\langle r \rangle$, and $\langle sr, r^2 \rangle$.
(d) If $H$ is a subgroup of $D_{16}$ that contains $\langle s \rangle$ as a proper subgroup, then $H$ must contain an element besides $s$ or the identity. Notice that if $r^i \in H$ then $sr^i \in H$ and conversely, so without loss of generality we may assume that $r^i \in H$ for some $0 < i < 8$. If $i = 1$, then clearly $H = D_{16}$. Similarly, if $i$ is any other odd number (the numbers relatively prime to 8), then some power of $r^i$ is equal to $r$, and hence $r$ is an element of $H$ from which we conclude $H = D_{16}$. The only other possibility would be $i = 2, 4$ or 6. Notice that the inverse of $r^2$ is $r^6$ so $\langle s, r^2 \rangle = \langle s, r^6$. Also if $r^2 \in H$ then $r^4 \in H$. We

summarize the situation by noting that all the subgroups containing $\langle s \rangle$ can be found in the nest of inclusions below:

$$\langle s \rangle \;\le\; \langle s, r^4 \rangle \;\le\; \langle s, r^2 \rangle \;\le\; D_{16}.$$

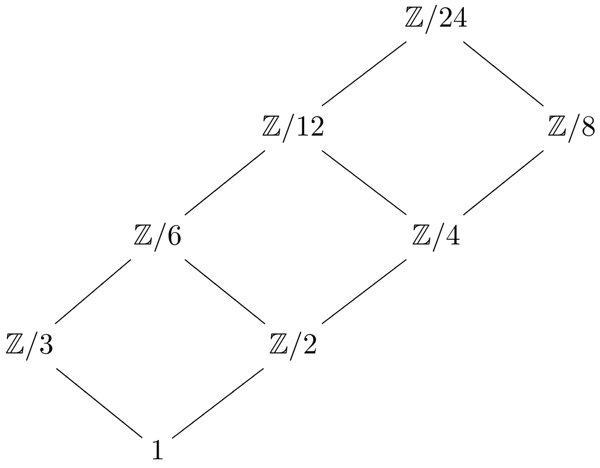
Of course we do not know which of these inclusions are proper. The leftmost one clearly is. Also note that $\langle s, r^2 \rangle$ does not contain any elements of the form $sr^i$ where $i$ is odd, so the rightmost inclusion is proper. Finally note that $r^2$ does not appear in $\langle s, r^4 \rangle$ so in fact all the inclusions are proper. Thus the proper subgroups of $D_{16}$ which contain $\langle s \rangle$ are $\langle s \rangle$, $\langle s, r^4 \rangle$, and $\langle s, r^2 \rangle$. You may check that these subgroups are isomorphic to $\mathbb{Z}/2, \mathbb{Z}/2 \oplus \mathbb{Z}/2$, and $D_8$ respectively.

**Chapter 2.5 Problem 9:** Draw the lattices of subgroups of the following groups:
(a) $\mathbb{Z}/16$ (b) $\mathbb{Z}/24$ (c) $\mathbb{Z}/48$.

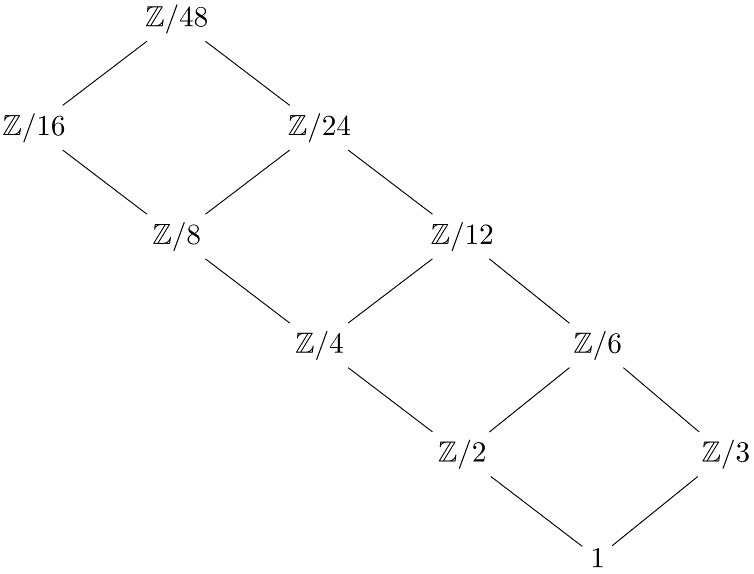
**Solution:**
(a)

$$\begin{tikzcd}
\mathbb{Z}/16 \arrow[d, no head] \\
\mathbb{Z}/8 \arrow[d, no head] \\
\mathbb{Z}/4 \arrow[d, no head] \\
\mathbb{Z}/2 \arrow[d, no head] \\
1
\end{tikzcd}$$

(b)



(c)



**Chapter 3.2 Problem 6:** Let $H \leq G$ and let $g \in G$. Prove that if the right coset $Hg$ equals *some* left coset of $H$ in $G$ then it equals the left coset $gH$ and $g$ must be in $N_G(H)$.

**Solution:** Notice that since $1 \in H$ and $1g = g$, the element $g$ is an element of $Hg$. Because $Hg = aH$ for some element $a \in G$, there must be an element $h$ such $g = ah$. Then we have $gH = (ah)H = a(hH) = aH = Hg$. The equation $gH = Hg$ is equivalent to the equation $gHg^{-1} = H$, or in other words, that $g{\in}N_G(H)$.

**Chapter 3.2 Problem 8:** Prove that if $H$ and $K$ are finite subgroups of $G$ whose orders are relatively prime then $H \cap K = \{1\}$.

**Solution:** Since $H$ and $K$ are subgroups of $G$, $H \cap K$ is a subgroup as well. Additionally, $H \cap K$ is a subset of $H$ and hence a subgroup of $H$. By Lagrange's theorem, we conclude that $|H \cap K|$ must divide $|H|$. Similarly, we conclude that $H \cap K$ is a subset of $K$ and that $|H \cap K|$ divides $|K|$. By hypothesis, the orders of $H$ and $K$ are relatively prime, so the only number which divides both $|H|$ and $|K|$ is one. So $|H \cap K| = 1$. The only group of order one is the trivial group.

**Chapter 3.2 Problem 11:** Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$ (do not assume $G$ is finite).

**Solution:** Suppose that $|G : K|$ and $|K : H|$ are finite. Fix a list $a_1, ..., a_k$ of coset representives of $K$ in $G$ and fix a list $b_1, ..., b_l$ of coset representatives of $H$ in $K$. We claim the products $a_ib_j$ represent distinct cosets of $H$ in $G$ and in fact represent all of them. This would verify the claim in the case when both $|G : K|$ and $|K : H|$ are finite.

To that end, suppose two elements $a_ib_j$ and $a_{i'}b_{j'}$ represent the same coset of $H$ in $G$. Then we'd have $(a_{i'}b_{j'})^{-1}a_ib_j{\in}H$ or in otherwords $b_{j'}^{-1}a_{i'}^{-1}a_ib_j{\in}H$. Since $H$ is a subset of $K$ we have $b_{j'}^{-1}a_{i'}^{-1}a_ib_j{\in}K$. Multiply this equation by $b_{j'}$ on the left and $b_j^{-1}$ on the right to see that $a_{i'}^{-1}a_i$ is an element of $b_{j'}Kb_j^{-1}$. The set $b_{j'}Kb_j^{-1}$ is actually equal to $K$ because both $b_j$ and $b_{j'}$ are elements of $K$. Hence we conclude that $a_{i'}^{-1}a_i$ lies in $K$, or in otherwords $a_i$ and $a_{i'}$ belong to the same coset of $K$ in $G$. Since the $a_i$'s came from a list of coset representatives of $K$ in $G$, the only way that this can happen is if $a_i = a_{i'}$. In this case, the original equation $(a_{i'}b_{j'})^{-1}a_ib_j{\in}H$ reduces to $b_{j'}^{-1}b_j{\in}H$ which implies that $b_j$ and $b_{j'}$ lie in the same coset of $H$. Again, the only way this is possible is for $b_j$ to equal $b_{j'}$. We have succeeded in verifying that if the pairs $(a_i, b_j)$ and $(a_{i'}, b_{j'})$ are distinct, then $a_ib_jH$ is a distinct coset from $a_{i'}b_{j'}H$.

Now suppose that $cH$ is some coset of $H$ in $G$. We aim to show that $cH = a_ib_jH$ for some $a_i$ and $b_j$ coming from the lists of coset representatives. To that end, consider the coset $cK$ in $G$. There is an element, say $a_i$ coming from our list of coset representatives of $K$ in $G$ such that $cK = a_iK$. This implies that the element $a_i^{-1}c$ lies in $K$. As such, we can consider the coset $a_i^{-1}cH$ which is a coset of $H$ that must lie in $K$ because $a_i^{-1}c \in K$. But then we can find an element, say $b_j$, coming from our list of coset representatives of $H$ in $K$ such that $a_i^{-1}cH = b_jH$. This implies though that $cH = a_ib_jH$. This is what we aimed to prove.

We still have to worry about the case when $|G : K|$ or $|K : H|$ is infinite. But it is easy to see that if one of two is infinite, then $|G : H|$ must be infinite too, so the equation still holds.

**Chapter 3.2 Problem 22:** Use Lagrange's Theorem in the multiplicative group $\left(\mathbb{Z}/n\right)^{\times}$ to prove *Euler's Theorem:*

$$a^{\phi(n)} \equiv 1 \mathrm{mod} n$$

for every integer $a$ relatively prime to $n$, where $\phi$ denotes Euler's $\phi$ function.

**Solution:** Recall that $\phi(n)$ is the number of positive numbers less than $n$ that are relatively prime to it. We claim that $|\left(\mathbb{Z}/n\right)^{\times}| = \phi(n)$. If this is true, then by Lagrange's theorem, the order of any subgroup of $\left(\mathbb{Z}/n\right)^{\times}$ divides $\phi(n)$. In particular, given any element $a \in \left(\mathbb{Z}/n\right)^{\times}$ we could consider the cyclic subgroup it generates. Then we'd have $|\langle a \rangle|$ divides $\phi(n)$. Also note that $|\langle a \rangle|$ is precisely the order of $a$, so in fact the order of $a$ divides $\phi(n)$. This means that $a^{\phi(n)} = (a^{\mathrm{ord}(a)})^{\frac{\phi(n)}{\mathrm{ord}(a)}} = 1^{\frac{\phi(n)}{\mathrm{ord}(a)}} = 1$. The condition $a^{\phi(n)} = 1$ in the group $\left(\mathbb{Z}/n\right)^{\times}$ is the same as the condition $a^{\phi(n)} \equiv 1 \mathrm{mod} n$.

It remains to show that $|\left(\mathbb{Z}/n\right)^{\times}| = \phi(n)$. This is done by showing that the elements $[a] \in \left(\mathbb{Z}/n\right)^{\times}$ are precisely those for which $a$ is relatively prime to $n$. If $a$ is not relatively prime to $n$, then there is an natural number $d > 1$ which divides $a$ and $n$. But if $a$ were in $\left(\mathbb{Z}/n\right)^{\times}$ there would be a number $b$ such that $ab = 1 \mathrm{mod} n$ or in otherwords $ab = 1 + ns$ for some $s \in \mathbb{N}$. But then we'd have $ab - ns = 1$. The number $d$ divides the lefthand side of this equation since it divides both $a$ and $n$. On the otherhand, it does not divide 1. Conversely we show that if $a$ is relatively prime to $n$ then $a \in \left(\mathbb{Z}/n\right)^{\times}$. This is a fact of basic number theory. I'm a little tired now and I'm gonna quit, but if you're curious about why this is true, come and see me or Sound.