Notes on Cosets, Quotient Groups, and Homomorphisms

10/28/04 Radford

Throughout $G$ is a (multiplicative) group and $H$ is a subgroup of $G$. Since all fully parenthesized expressions for $a_1 \cdots a_n$, where $a_1, \ldots, a_n \in G$, yield the same product, we will tend to omit parentheses in product expressions.

1 Cosets

A left coset of $H$ in $G$ is a subset of $G$ of the form

$$aH = \{ah \mid h \in H\},$$

where $a \in G$, and a right coset of $H$ in $G$ is a subset of $G$ of the form

$$Ha = \{ha \mid h \in H\},$$

were $a \in G$. Cosets play a very important role in the theory of groups. We begin by listing three of their basic properties.

(1) $a \in aH$ for all $a \in G$.

This follows since $e \in H$ and $a = ae \in aH$ for all $a \in G$.

(2) For $a,b \in G$ either $aH = bH$ or $aH \cap bH = \emptyset$.

To see this, suppose that $a,b \in G$ and $aH \cap bH \neq \emptyset$. We need only show that $aH = bH$.

Since $aH \cap bH \neq \emptyset$ there is an $x \in aH \cap bH$. Since $x \in aH$ we have $x = ah$ for some $h \in H$. Likewise, since $x \in bH$, there is an $h' \in H$ such that $x = bh'$. Thus for $h'' \in H$ we calculate

$$ah'' = ahh^{-1}h'' = (ah)h^{-1}h'' = bh'h^{-1}h'' \in bH;$$
the last product belongs to $bH$ since $h',h,h'' \in H$ and $H$ is a subgroup of $G$. We have shown that $aH \subseteq bH$. Since $bH \cap aH = aH \cap bH \neq \emptyset$, by the preceding argument $bH \subseteq aH$. Putting the two inclusions together gives $aH = bH$.

(3) For $a \in G$ then function $f_a : H \to aH$ defined by $f_a(h) = ah$ for all $h \in H$ is a set bijection.

By definition of left coset $f_a$ is onto. By cancelation $f_a$ is one-one.

Since the inverse of a set bijection is a set bijection, and the composite of set bijections is a set bijection, $f = f_b \circ (f_a)^{-1} : aH \to bH$ is a set bijection.

As a consequence:

(4) For $a, b \in G$ the left cosets $aH$ and $bH$ have the same cardinality.

Observe that $f(ah) = bh$ for all $h \in H$.

By (1) the set $G$ is the union of the distinct left cosets of $H$. By (2) distinct left cosets of $H$ are disjoint. Therefore the distinct left cosets of $H$ in $G$ partition $G$. Since any two left cosets of $H$ in $G$ have the same cardinality by (4) we have:

**Theorem 1** Let $G$ be a finite group and suppose that $H$ is a subgroup of $G$. Then $|H|$ divides $|G|$. Furthermore the number of distinct left cosets of $H$ in $G$ is $|G|/|H|$. □

The reader is left with the exercise of formulating and proving analogs of (1)–(4) for right cosets of $H$ in $G$. When $G$ is finite note that the number of right cosets of $H$ in $G$ is $|G|/|H|$. Also.

The preceding theorem, without the number of cosets statement, is Lagrange’s Theorem. It has enormous implications for the theory of finite groups. One consequence:

**Corollary 1** Let $G$ be a finite group. Then:

a) $|a|$ divides $|G|$ for all $a \in G$.

b) If $|G|$ is prime then $G = \langle a \rangle$ for all $a \in G \setminus e$.

**Proof:** Since $|a| = |\langle a \rangle|$ for all $a \in G$, part b) follows from part a) and part a) follows from the preceding theorem. □
2 Normal Subgroups

Generally left cosets of $H$ in $G$ are not right cosets of $H$ in $G$. When they are can be expressed in several important ways. First a technicality.

For $a, b \in G$ we define

$$aHb = \{ahb \mid h \in H\}.$$  

**Theorem 2** Let $G$ be a group and $H$ be a subgroup of $G$. Then the following are equivalent:

a) The set of left cosets of $H$ in $G$ is the set of right cosets of $H$ in $G$.

b) $aH = Ha$ for all $a \in G$.

c) $aHa^{-1} \subseteq H$ for all $a \in G$.

d) $aHa^{-1} = H$ for all $a \in G$.

**Proof:** To show that all statements are equivalent it suffices to show that a) $\implies$ b) $\implies$ c) $\implies$ d) $\implies$ a).

a) $\implies$ b). Suppose that the set of left cosets of $H$ in $G$ is the set of right cosets of $H$ in $G$. Let $a \in G$. Then $Ha = bH$ for some $b \in G$. Now $a = ea \in Ha = bH$ by assumption. Since $a \in aH$ by (1), and $a \in bH$ we deduce that $aH = bH$ by (2). Therefore $aH = bH = Ha$.

b) $\implies$ c). Suppose that $aH = Ha$ for all $a \in G$ and let $a \in G$. Then

$$aHa^{-1} = (aH)a^{-1} = (Ha)a^{-1} = Haa^{-1} = He = H$$

which actually shows that $aHa^{-1} = H$. In particular $aHa^{-1} \subseteq H$.

c) $\implies$ d). Suppose that $aHa^{-1} \subseteq H$ for all $a \in G$ and let $a \in G$. By assumption $xHx^{-1} \subseteq H$ for all $x \in G$; thus $aHa^{-1} \subseteq H$ and $a^{-1}Ha = a^{-1}H(a^{-1})^{-1} \subseteq H$. The latter implies

$$H = eHe = aa^{-1}Ha^{-1}a = a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1}.$$ 

Thus $aHa^{-1} \subseteq H \subseteq aHa^{-1}$ which means that $aHa^{-1} = H$.

d) $\implies$ a). Suppose that $aHa^{-1} = H$ for all $a \in G$ and let $a \in G$. Then

$$aH = aHe = aHa^{-1}a = (aHa^{-1})a = Ha.$$
Therefore the set of left cosets of $H$ in $G$ is the set of all right cosets of $H$ in $G$. □

If $H$ satisfies any one (hence all) of the conditions of the preceding theorem the $H$ is a normal subgroup of $G$. Observe that $G$ and $(e)$ are always normal subgroups of $G$. If $H \subseteq Z(G)$ then $H$ is normal since $aha^{-1} = haa^{-1} = he = h$ for all $a \in G$ and $h \in Z(G)$. In particular all subgroups of an abelian group are normal.

When $H$ is normal all left cosets of $H$ in $G$ form a group.

**Proposition 1** Let $G$ be a group and suppose that $H$ is a normal subgroup of $G$. Then the set of left cosets of $H$ in $G$ is a group, denoted by $G/H$, where

\[(aH)(bH) = abH\]

for all $a, b \in G$.

**Proof:** First of all coset multiplication is well-defined. Let $a, a', b, b' \in G$ and suppose that $aH = a'H$, $bH = b'H$. We need to show that $abH = a'b'H$.

Since $aH = Ha$ it follows that $a = ae \in aH = a'H$. Therefore $a = a'h$ for some $h \in H$. Since $Hb = bH$ it follows that $hb = b'h'$ for some $h' \in H$. Combining equations we calculate

\[ab = (a'h)b = a'(hb) = a'(b'h') = (a'b')h' \in a'b'H.\]

Since $ab \in a'b'H$ we conclude that $abH = a'b'H$ by (2). We have shown the multiplication rule is well-defined.

Let $a, b, c \in G$. Then associativity follows by

\[((aH)(bH))(cH) = (abH)cH = (ab)(cH) = a(bc)H = (aH)((bH)(cH)).\]

The coset $eH = H$ is the neutral element of $G/H$ since

\[(aH)(eH) = aeH = aH = eaH = (eH)(aH)\]

for all $a \in G$. For $a \in G$ the calculation

\[(aH)(a^{-1}H) = aa^{-1}H = eH = a^{-1}aH = (a^{-1})H(aH)\]

shows that $a^{-1}H$ is an inverse of $aH$. □

The group $G/H$ of Proposition 1 is call a **quotient group**.
3 Homomorphisms

Suppose that $f : X \rightarrow Y$ is a function. For a subset $Z$ of $X$ we let

$$f(Z) = \{f(x) \mid x \in Z\} \subseteq Y$$

denote the image of $Z$ under $f$ and for a subset $W$ of $Y$ we let

$$f^{-1}(W) = \{x \in X \mid f(x) \in W\} \subseteq X$$

denote the preimage of $W$ under $f$. Observe that if $f$ is one-one and onto then $f^{-1}(W)$ is the image of $W$ under the inverse function $f^{-1}$.

Let $G'$ be a group also and suppose that $f : G \rightarrow G'$ is a function. Then $f$ is a homomorphism if

$$f(ab) = f(a)f(b)$$

for all $a, b \in G$. If $f$ is a homomorphism then $f$ is called an isomorphism if $f$ is one-one and onto. If $G = G'$ and $f : G \rightarrow G$ is an isomorphism, then $f$ is called an automorphism of $G$.

There are many examples of group homomorphisms. One of the more important ones from a theoretical point of view arises from a normal subgroup $H$ of $G$. The quotient group $G/H$ of Proposition 1 is a group. Let $\pi : G \rightarrow G/H$ be defined by $\pi(a) = aH$ for all $a \in G$. The calculation

$$\pi(ab) = abH = (aH)(bH) = \pi(a)\pi(b)$$

for all $a, b \in G$ shows that $\pi$ is a homomorphism.

Suppose that $f : G \rightarrow G'$ is a homomorphism. Then

$$\text{Ker } f = \{a \in G \mid f(a) = e'\} \quad \text{and} \quad \text{Im } f = f(G).$$

are the kernel of $f$ and the image of $f$ respectively. Observe that

$$\text{Ker } f = f^{-1}\{e'\}$$

and is thus a preimage.

**Theorem 3** Let $G, G'$ be groups and suppose that $f : G \rightarrow G'$ is a homomorphism. Then:

a) $f(e) = e'$
b) $f(a^n) = f(a)^n$ for all $a \in G$ and $n \in \mathbb{Z}$. In particular $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$.

c) $|f(a)|$ divides $|a|$ for all $a \in G$ of finite order.

d) Let $a, b \in G$. Then $f(a) = f(b)$ if and only if $b \in a(\text{Ker } f)$.

**Proof:** We first show part a). Since $f(e)^2 = f(e)f(e) = f(ee) = f(e)$, and the equation $x^2 = x$ in a group has a unique solution which is the neutral element, part a) follows.

Let $a \in G$. Part b) splits into two cases: $n$ non-negative and $n$ negative. The first is done by induction. By part a) note that $f(a^0) = f(e) = e' = f(a)^0$. Suppose that $n > 0$ and $f(a^{n-1}) = f(a)^{n-1}$. Then

$$f(a^n) = f(aa^{n-1}) = f(a)f(a^{n-1}) = f(a)^n f(a)^{n-1} = f(a)^n.$$  

Therefore $f(a^n) = f(a)^n$ for all $n \geq 0$ by induction on $n$.

The second case reduces to the first. Since $e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$, and likewise $e' = f(a^{-1})f(a)$, it follows that $f(a^{-1}) = f(a)^{-1}$. Suppose that $n < 0$. Then $-n > 0$ and $a^n = (a^{-1})^{-n}$. Using the first case we have

$$f(a^n) = f((a^{-1})^{-n}) = f(a^{-1})^{-n} = (f(a)^{-1})^n = f(a)^n.$$  

which completes our proof of part b).

Suppose $a \in G$ has finite order $n$. Then $f(a^n) = f(a^n) = f(e) = e'$ by parts b) and a). Therefore $f(a)$ has finite order $m$ and $m$ divides $n$. We have shown part c).

As for part d), let $a, b \in G$. Suppose first of all that $b \in a(\text{Ker } f)$. Then $b = ah$ for some $h \in \text{Ker } f$. Therefore $f(b) = f(ah) = f(a)f(h) = f(a)e' = f(a)$.

Conversely, suppose that $f(a) = f(b)$ and set $h = a^{-1}b$. Then $b = aa^{-1}b = ah$. Since

$$f(b)e' = f(b) = f(ah) = f(a)f(h) = f(b)f(h)$$

it follows that $e' = f(h)$ be right cancelation. Therefore $b \in a(\text{Ker } f)$. This completes our proof of part d). □

Suppose that $f : G \longrightarrow G'$ is a group homomorphism. Then $f(e) = e'$ by part a) of the preceding theorem. Thus $e \in \text{Ker } f$. The homomorphism $f$ is one-one if and only if $\text{Ker } f$ is as small as possible.
Corollary 2 Let $G, G'$ be groups and suppose that $f : G \longrightarrow G'$ is a homomorphism. Then $f$ is one-one if and only if Ker = \{e\}.

Proof: Suppose that $f$ is one-one and let $a \in$ Ker $f$. Then $f(a) = e'$. Since $f(e) = e'$ also necessarily $a = e$. We have shown that Ker $f = \{e\}$.

Conversely, suppose that Ker $f = \{e\}$. Let $a, b \in G$ and $f(a) = f(b)$. Then by part d) of Theorem 3 we have $b \in a($Ker $f) = a$\{e\} = \{ae\} = \{a\}$ which implies $b = a$. Thus $f$ is one-one. $\square$

Images and preimages of subgroups under a homomorphism are subgroups.

Theorem 4 Let $G, G'$ be groups and suppose that $f : G \longrightarrow G'$ is a homomorphism.

a) If $H$ is a subgroup of $G$ then $f(H)$ is a subgroup of $G'$. In particular Im $f = f(G)$ is a subgroup of $G'$.

b) If $H$ is a normal subgroup of $G$ then $f(H)$ is a normal subgroup of $f(G)$.

c) If $K$ is a subgroup of $G'$ then $f^{-1}(K)$ is a subgroup of $G$.

d) If $K$ is a normal subgroup of $G'$ then $f^{-1}(K)$ is a normal subgroup of $G$. In particular Ker $f = f^{-1}(\{e'\})$ is a normal subgroup of $G$.

Proof: Let $H$ be a subgroup of $G$. Then $f(H) \neq \emptyset$ since $H \neq \emptyset$. We will show that $f(H)$ is a subgroup of $G'$ by the 1-Step Subgroup Test.

Suppose that $a, b \in f(H)$. Then $a = f(h)$ and $b = f(k)$ for some $h, k \in H$. Since $H$ is a subgroup of $G$, by the 1-Step Subgroup Test $h^{-1}k \in H$. We use part b) of Theorem 3 to show that

$$a^{-1}b = f(h)f(k)^{-1} = f(h)f(k^{-1}) = f(hk^{-1}) \in f(H).$$

Thus $f(H)$ is a subgroup of $G'$ by the 1-Step Subgroup Test. We have shown part a).

By part a) the image $f(G)$ of $f$ is a subgroup of $G'$. Since $H \subseteq G$ we have $f(H) \subseteq f(G)$. Therefore $f(H)$ is a subgroup of $f(G)$. To show that $f(H)$ is a normal subgroup of $f(G)$ let $a \in f(H)$ and $b \in f(G)$. Then $a = f(h)$ for
some $h \in H$ and $b = f(g)$ for some $g \in G$. Since $H$ is a normal subgroup of $G$ the product $ghg^{-1} \in H$ by Theorem 2. By part b) of Theorem 3 again

$$bab^{-1} = f(g)f(h)f(g)^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1}) \in f(H).$$

Therefore $f(H)$ is a normal subgroup of $f(G)$ by Theorem 2 again. We have shown part b).

As for part c), we note that $e \in f^{-1}(K)$ as $f(e) = e' \in K$. Thus $f^{-1}(K) \neq \emptyset$. We show that $f^{-1}(K)$ is a subgroup of $G$ by the 1-Step Subgroup Test.

Suppose $a, b \in f^{-1}(K)$. Then $f(a), f(b) \in K$ by definition. Thus

$$f(a^{-1}b) = f(a^{-1})f(b) = f(a)^{-1}f(b) \in K$$

by the 1-Step Subgroup Test. Thus $a^{-1}b \in f^{-1}(K)$. We have shown that $f^{-1}(K)$ is a subgroup of $G$. The fact that $f^{-1}(K)$ is normal when $K$ is normal is left as a small exercise for the reader. □

**Proposition 2** Let $G, G'$ be groups and suppose that $f : G \rightarrow G'$ is an onto homomorphism.

a) If $G$ is abelian then $G'$ is abelian.

b) $f(<a>) = <f(a)>$ for all $a \in G$. In particular if $G$ is cyclic then $G'$ is cyclic.

**Proof:** Two elements of $G'$ can be written as $f(a)$ and $f(b)$ for some $a, b \in G$ since $f$ is onto. Since $G$ is abelian $f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$. We have shown part a).

The equation of part b) follows by part d) of Theorem 3. Since $f$ is onto, the subsequent statement follows form the equation. □

By part d) of Theorem 4 the kernel of a homomorphism $f : G \rightarrow G'$ is a normal subgroup of $G$. Suppose that $G$ is a group and $H$ is a normal subgroup of $G$. We have noted at the beginning of this section that $\pi : G \rightarrow G/H$ defined by $\pi(a) = aH$ for all $a \in G$ is a homomorphism. Note that $a \in \text{Ker} \pi$ if and only if $\pi(a) = eH$ if and only if $aH = eH$ if and only if $a \in eH = H$. Therefore $H = \text{Ker} \pi$. We have shown that:

(5) Kernels and normal subgroups are one in the same.
We end this section with the relationship between the image of a homomorphism and its kernel. Let \( f : G \rightarrow G' \) be a homomorphism. Since \( \text{Im } f = F(G) \) is a subgroup of \( G' \) by part a) of Theorem 4, we may think of \( f \) as a function from \( G \) to \( f(G) \). Thus we will assume that \( f \) is onto. Recall that \( H = \text{Ker } f \) is a normal subgroup of \( G \) by part d) of Theorem 4.

We show that \( F : G/H \rightarrow G' \) defined by

\[
F(aH) = f(a)
\]

for all \( a \in G \) is a well-defined isomorphism. To show well-defined, let \( a, b \in G \) and suppose that \( aH = bH \). Since \( b \in bH = aH = a(\text{Ker } f) \) it follows by part d) of Theorem 3 that \( f(a) = f(b) \). Therefore \( F \) is a well-defined function.

Since \( f \) is onto \( F \) is onto. Suppose that \( a, b \in G \) and \( F(aH) = F(bH) \). Then \( f(a) = f(b) \) by definition. By part d) of Theorem 3 again we have \( b \in a\text{Ker } f = aH \). Therefore \( aH = bH \) by (2). We have shown that \( F \) is one-one. To complete our proof that \( F \) is an isomorphism we need only show that

\[
F((aH)(bH)) = F(abH) = f(ab) = f(a)f(b) = F(aH)F(bH)
\]

for all \( a, b \in G \). Note that the composite \( G \xrightarrow{\pi} G/H \xrightarrow{F} G' \) is \( f \) as \( (F \circ \pi)(a) = F(\pi(a)) = F(aH) = f(a) \) for all \( a \in G \). In terms of diagrams

\[
\begin{array}{c}
G/H \xrightarrow{F} G' \\
\pi \\
G \xrightarrow{f}
\end{array}
\]

where \( F \circ \pi = f \). The First Isomorphism Theorem is a codification of the preceeding discussion.

Regarding isomorphic groups as equal, we would equate \( G/H \) and \( G' = \text{Im } f \) and thus equate \( f \) and \( \pi \). From this point of view every homomorphic image has the form \( G/H \) and every homomorphism has the form \( \pi \).