quotient group

Canonical name	QuotientGroup
Date of creation	2013-03-22 12:04:06
Last modified on	2013-03-22 12:04:06
Owner	azdbacks4234 (14155)
Last modified by	azdbacks4234 (14155)
Numerical id	35
Author	azdbacks4234 (14155)
Entry type	Definition
Classification	msc 20-00
Synonym	factor group
Synonym	quotient
Related topic	Group
Related topic	NormalSubgroup
Related topic	Subgroup
Related topic	EquivalenceRelation
Related topic	Coset
Related topic	NaturalProjection
Defines	left congruence modulo a subgroup
Defines	right congruence modulo a subgroup
Defines	index

Before defining quotient groups, some preliminary definitions must be introduced and a few established.

Given a group G and a subgroup H of G, the http://planetmath.org/node/122relation $\sim_L$ on G defined by $a \sim_L b$ if and only if $b^{-1}a \in H$ is called *left congruence modulo* H; similarly the relation defined by $a \sim_R b$ if and only if $ab^{-1} \in H$ is called *congruence modulo* H (observe that these two relations coincide if G is abelian).

Proposition. *Left (resp. right) congruence modulo H is an equivalence relation on G.*

Proof. We will only give the proof for left congruence modulo H, as the for right congruence modulo H is analogous. Given $a \in G$, because H is a subgroup, H contains the identity e of G, so that $a^{-1}a = e \in H$; thus $a \sim_L a$, so $\sim_L$ is http://planetmath.org/node/1644reflexive. If $b \in G$ satisfies $a \sim_L b$, so that $b^{-1}a \in H$, then by the of H under the formation of inverses, $a^{-1}b = (b^{-1}a)^{-1} \in H$, and $b \sim_L a$; thus $\sim_L$ is symmetric. Finally, if $c \in G$, $a \sim_L b$, and $b \sim_L c$, then we have $b^{-1}a, c^{-1}b \in H$, and the closure of H under the binary operation of G gives $c^{-1}a = (c^{-1}b)(b^{-1}a) \in H$, so that $a \sim_L c$, from which it follows that $\sim_L$ is http://planetmath.org/node/1669transitive, hence an equivalence relation. □

It follows from the preceding that G is partitioned into mutually disjoint, non-empty equivalence classes by left (resp. right) congruence modulo H, where $a, b \in G$ are in the same equivalence class if and only if $a \sim_L b$ (resp. $a \sim_R b$); focusing on left congruence modulo H, if we denote by $\bar{a}$ the equivalence class containing a under $\sim_L$, we see that

$$\begin{aligned}
\bar{a} &= \{b \in G \mid b \sim_L a\} \\
&= \{b \in G \mid a^{-1}b \in H\} \\
&= \{b \in G \mid b = ah \text{ for some } h \in H\} = \{ah \mid h \in H\}.
\end{aligned}$$

Thus the equivalence class under $\sim_L$ containing a is simply the left coset aH of H in G. Similarly the equivalence class under $\sim_R$ containing a is the right coset Ha of H in G (when the binary operation of G is written additively, our notation for left and right cosets becomes $a+H = \{a+h \mid h \in H\}$ and $H + a = \{h + a \mid h \in H\}$). Observe that the equivalence class under either $\sim_L$ or $\sim_R$ containing e is $eH = H$. The *index* of H in G, denoted by

$|G : H|$, is the cardinality of the set G/H (read "G modulo H" or just "G mod H") of left cosets of H in G (in fact, one may demonstrate the existence of a bijection between the set of left cosets of H in G and the set of right cosets of H in G, so that we may well take $|G : H|$ to be the cardinality of the set of right cosets of H in G).

We now attempt to impose a group on G/H by taking the of the left cosets containing the elements a and b, respectively, to be the left coset containing the element ab; however, because this definition requires a choice of left coset representatives, there is no guarantee that it will yield a well-defined binary operation on G/H. For the of left coset to be well-defined, we must be sure that if $a'H = aH$ and $b'H = bH$, i.e., if $a' \in aH$ and $b' \in bH$, then $a'b'H = abH$, i.e., that $a'b' \in abH$. Precisely what must be required of the subgroup H to ensure the of the above condition is the content of the following :

Proposition. *The rule $(aH, bH) \mapsto abH$ gives a well-defined binary operation on G/H if and only if H is a normal subgroup of G.*

Proof. Suppose first that of left cosets is well-defined by the given rule, i.e, that given $a' \in aH$ and $b' \in bH$, we have $a'b'H = abH$, and let $g \in G$ and $h \in H$. Putting $a = 1$, $a' = h$, and $b = b' = g^{-1}$, our hypothesis gives $hg^{-1}H = eg^{-1}H = g^{-1}H$; this implies that $hg^{-1} \in g^{-1}H$, hence that $hg^{-1} = g^{-1}h'$ for some $h' \in H$. on the left by g gives $ghg^{-1} = h' \in H$, and because g and h were chosen arbitrarily, we may conclude that $gHg^{-1} \subseteq H$ for all $g \in G$, from which it follows that $H \trianglelefteq G$. Conversely, suppose H is normal in G and let $a' \in aH$ and $b' \in bH$. There exist $h_1, h_2 \in H$ such that $a' = ah_1$ and $b' = bh_1$; now, we have

$$a'b' = ah_1bh_2 = a(bb^{-1})h_1bh_2 = ab(b^{-1}h_1b)h_2,$$

and because $b^{-1}h_1b \in H$ by assumption, we see that $a'b' = abh$, where $h = (b^{-1}hb)h_2 \in H$ by the closure of H under in G. Thus $a'b' \in abH$, and because left cosets are either disjoint or equal, we may conclude that $a'b'H = abH$, so that multiplication of left cosets is indeed a well-defined binary operation on G/H. $\square$

The set G/H, where H is a normal subgroup of G, is readily seen to form a group under the well-defined binary operation of left coset multiplication (the of each group follows from that of G), and is called a *quotient* or *factor group* (more specifically the *quotient of G by H*). We conclude with several examples of specific quotient groups.

Example. A standard example of a quotient group is $\mathbb{Z}/n\mathbb{Z}$, the quotient of the of integers by the cyclic subgroup generated by $n \in \mathbb{Z}^+$; the order of $\mathbb{Z}/n\mathbb{Z}$ is n, and the distinct left cosets of the group are $n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$.

Example. Although the group Q_8 is not abelian, each of its subgroups its normal, so any will suffice for the formation of quotient groups; the quotient $Q_8/\langle -1\rangle$, where $\langle -1\rangle = \{1,-1\}$ is the cyclic subgroup of Q_8 generated by -1, is of order 4, with elements $\langle -1\rangle, i\langle -1\rangle = \{i,-i\}, k\langle -1\rangle = \{k,-k\}$, and $j\langle -1\rangle = \{j,-j\}$. Since each non-identity element of $Q_8/\langle -1\rangle$ is of order 2, it is isomorphic to the Klein 4-group V. Because each of $\langle i\rangle$, $\langle j\rangle$, and $\langle k\rangle$ has order 4, the quotient of Q_8 by any of these subgroups is necessarily cyclic of order 2.

Example. The center of the dihedral group D_6 of order 12 (with `http://planetmath.org/node/21` $\langle r,s \mid r^6 = s^2 = 1, r^{-1}s = sr\rangle$) is $\langle r^3\rangle = \{1,r^3\}$; the elements of the quotient $D_6/\langle r^3\rangle$ are $\langle r^3\rangle$, $r\langle r^3\rangle = \{r,r^4\}$, $r^2\langle r^3\rangle = \{r^2,r^5\}$, $s\langle r^3\rangle = \{s,sr^3\}$, $sr\langle r^3\rangle = \{sr,sr^4\}$, and $sr^2\langle r^3\rangle = \{sr^2,sr^5\}$; because

$$sr^2\langle r^3\rangle r\langle r^3\rangle = sr^3\langle r^3\rangle = s\langle r^3\rangle \neq sr\langle r^3\rangle = r\langle r^3\rangle sr^2\langle r^3\rangle,$$

$D_6/\langle r^3\rangle$ is non-abelian, hence must be isomorphic to S_3.