Queen Mary
University of London

MAS 305 **Algebraic Structures II**

Notes 2 **Autumn 2006**

Group Theory

A *group* is a set G with a binary operation $\circ$ such that

closure for all g, h in G, $g \circ h \in G$;

associativity for all g, h, k in G, $(g \circ h) \circ k = g \circ (h \circ k)$;

identity there is an element 1_G in G with $1_G \circ g = g = g \circ 1_G$ for all g in G;

inverses for all g in G, there is an element g^{-1} such that $g \circ g^{-1} = 1_G = g^{-1} \circ g$.

A group is *commutative*, or *Abelian*, if $g \circ h = h \circ g$ for all g, h in G.

In an Abelian group we often write $g \circ h$ as $g + h$. Otherwise we usually write $g \circ h$ as gh. Associativity implies that there is no doubt about what ghk means.

The *order* of a group G is $|G|$, the number of elements in G. G is said to be finite if $|G|$ is finite, infinite otherwise.

Examples

(a) $(\mathbb{Z}, +)$ is an infinite Abelian group.

(b) $(\mathbb{Q} \setminus \{0\}, \times)$ is an infinite Abelian group.

(c) $\mathrm{GL}(n, \mathbb{R})$ consists of all invertible $n \times n$ matrices with real entries. Under matrix multiplication, it is an infinite nonAbelian group. It is called the *general linear* group of dimension n over $\mathbb{R}$.

(d) Similarly, if p is prime, $\mathrm{GL}(n, p)$ consists of all invertible $n \times n$ matrices with entries in $\mathbb{Z}_p$.

(e) S_n is the group of all permutations of $\{1,2,\ldots,n\}$. It is called the *symmetric* group of degree n. The operation is composition of functions. We write permutations as functions on the *right*, so gh means "do g and then do h". If $n = 5$ and

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

then $1g = 2$ and the cycle form of g is $(123)(45)$. If, in addition, $h = (24)$ then $gh = (14523)$.

(f) D_{2n} is the group of all rotations and reflections of the regular polygon with n sides that leave the polygon occupying the same space. It is called the *dihedral* group of order $2n$.

It follows from the axioms that

(a) the identity element is unique;

(b) each element has a unique inverse;

(c) $(gh)^{-1} = h^{-1}g^{-1}$;

(d) (**cancellation**) if $gh = gk$ then $h = k$, and if $gh = kh$ then $g = k$;

(e) (**general associativity**) the product $g_1g_2\ldots g_n$ is well defined without parentheses.

Subgroups

Definition A subset H of a group G is a *subgroup* of G if it is a group under the same operation.

Notation We write $H \leqslant G$ to show that H is a subgroup of G, and $H < G$ to show that H is a subgroup of G but $H \neq G$.

The Subgroup Test A subset H of G is a subgroup of G if and only if

(a) H is not empty, and

(b) whenever h_1 and h_2 are in H then $h_1^{-1}h_2 \in H$.

Usually the easiest way of verifying (a) is to show that $1_G \in H$.

If $H \leqslant G$ then $1_H = 1_G$.
$\{1_G\}$ is always a subgroup of G, called the *trivial* subgroup, often written as 1.
G is a subgroup of itself.

Lemma If H and K are subgroups of G, then so is $H \cap K$. In fact, the intersection of any non-empty collection of subgroups is a subgroup of G.

Proof Exercise.

Powers

If g is an element of a group G and m is a positive integer then

$$\begin{array}{rll} g^m & \text{denotes} & \underbrace{g \circ g \circ g \circ \cdots \circ g}_{m \text{ times}} \\ g^0 & \text{denotes} & 1_G \\ g^{-m} & \text{denotes} & \left(g^{-1}\right)^m. \end{array}$$

Then $g^n \circ g^m = g^{n+m} = g^m \circ g^n$ for all integers n and m.

Definition If $g, g^2, \ldots, g^n, \ldots$ are all distinct then g has *infinite order*. Otherwise, the *order* of g is the smallest positive integer n with $g^n = 1_G$.

If g has order n then $g^m = 1_G$ if and only if n divides m.

Theorem If G is a group and $g \in G$ then $\{g^n : n \in \mathbb{Z}\}$ is a subgroup of G.

This subgroup is written $\langle g \rangle$, and called the *subgroup generated by* g. Any (sub-) group of this form is called *cyclic*. The order of the subgroup $\langle g \rangle$ is equal to the order of the element g.

Example In D_{2n}, let r be the rotation clockwise through $2\pi/n$. Then r^m is rotation through $2m\pi/n$ and so r has order n. Therefore $\langle r \rangle$ is a cyclic subgroup of order n.

Cosets

Let H be a subgroup of a group G. Define $\sim_R$ on G by

$$x \sim_R y \iff yx^{-1} \in H.$$

This is an equivalence relation, as we now check.

(a) If $x \in G$ then $xx^{-1} = 1_G \in H$ so $x \sim_R x$: hence $\sim_R$ is reflexive.

(b) If $x \sim_R y$ then $yx^{-1} \in H$ so $\left(yx^{-1}\right)^{-1} \in H$ so $xy^{-1} \in H$ so $y \sim_R x$: hence $\sim_R$ is symmetric.

(c) If $x \sim_R y$ and $y \sim_R z$ then $yx^{-1} \in H$ and $zy^{-1} \in H$ so $(zy^{-1})(yx^{-1}) \in H$ so $zx^{-1} \in H$ so $x \sim_R z$: hence $\sim_R$ is transitive.

The equivalence classes of $\sim_R$ are called the *right cosets* of H in G. The right coset containing x is

$$\begin{aligned}
[x] &= \{y \in G : y \sim_R x\} \\
&= \left\{y \in G : yx^{-1} \in H\right\} \\
&= \left\{y \in G : yx^{-1} = h \text{ for some } h \text{ in } H\right\} \\
&= \{y \in G : y = hx \text{ for some } h \text{ in } H\} \\
&= \{hx : h \in H\},
\end{aligned}$$

which is written Hx.

Sometimes it is helpful to think of the right coset containing x as simply the equivalence class containing x; at other times, it is helpful to think of it as the set of all elements hx for h in H.

Similarly, define $\sim_L$ by $x \sim_L y \iff x^{-1}y \in H$. This is also an equivalence relation (proof: exercise). Its equivalence classes have the form $\{xh : h \in H\} = xH$ and are called *left cosets*.

Theorem There is a bijection from the set of right cosets of H to the set of left cosets of H, so there are the same number of cosets of each type.

Proof Define f from the set of right cosets to the set of left cosets by

$$f(Hx) = x^{-1}H.$$

We must show that

(a) f is well defined;

(b) f is one-to-one;

(c) f is onto.

Part (a) is the standard problem when defining functions or operations on equivalence classes: we must ensure that our definition does not depend on the the element which we have used to name the class. Parts (b) and (c) show that f is a bijection.

(a) If $Hx = Hy$ then $x \sim_R y$ so $yx^{-1} \in H$ so $(y^{-1})^{-1}(x^{-1}) \in H$ so $y^{-1} \sim_L x^{-1}$ so $y^{-1}H = x^{-1}H$.

(b)

$$\begin{aligned} f(Hx) = f(Hy) &\Rightarrow x^{-1}H = y^{-1}H \\ &\Rightarrow y^{-1} = x^{-1}h \qquad \text{for some } h \text{ in } H \\ &\Rightarrow y = h^{-1}x \in Hx \\ &\Rightarrow Hy = Hx. \end{aligned}$$

(c) Given the left coset zH, $f(Hz^{-1}) = zH$. $\square$

Definition The number of right (or of left) cosets of H in G is the *index* of H in G, written $|G:H|$.

Lagrange's Theorem If G is a finite group and $H \leqslant G$ then $|G| = |H| \times |G:H|$.

Proof Fix an element x in G. Define $f{:}H \to Hx$ by $f(h) = hx$. Clearly, f is onto. If $f(h_1) = f(h_2)$ then $h_1x = h_2x$ so $h_1 = h_2$ (by cancellation); therefore f is one-to-one. Hence f is a bijection, so $|Hx| = |H|$.

There are $|G:H|$ cosets, each of size $|H|$, so $|G:H| \times |H| = |G|$. $\square$

Corollary In a finite group G, the order of each subgroup, and the index of each subgroup, both divide the order of G.

Corollary If G is finite and $g \in G$ then the order of g divides the order of G.

Proof Apply Lagrange's Theorem to the subgroup $\langle g \rangle$. $\square$

Normal subgroups

Definition A subgroup H of G is a *normal* subgroup of G if $g^{-1}hg \in H$ for all h in H and all g in G.

Notation We write $H \trianglelefteq G$ to indicate that H is normal subgroup of G, and $H \triangleleft G$ to show that H is a normal subgroup of G other than G itself.

Lemma The following are equivalent.

(a) $H \trianglelefteq G$;

(b) for every g in G, $\left\{g^{-1}hg : h \in H\right\} = H$;

(c) for all g in G, $gH = Hg$, that is, every left coset is a right coset.

Proof Write $g^{-1}Hg = \left\{g^{-1}hg : h \in H\right\}$. We show that (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (a).

(a) $\Longrightarrow$ (b) Choose any element g in G. By (a), $g^{-1}Hg \subseteq H$. Also by (a), $gHg^{-1} \subseteq H$. Therefore $g^{-1}\left(gHg^{-1}\right)g \subseteq g^{-1}Hg$. But $g^{-1}\left(gHg^{-1}\right)g = \left\{g^{-1}ghg^{-1}g : h \in H\right\} = H$, so $H \subseteq g^{-1}Hg$. Now each of H and $g^{-1}Hg$ is a subset of the other, so $H = g^{-1}Hg$.

(b) $\Longrightarrow$ (c) Let $g \in G$. Then (b) $\Rightarrow g^{-1}Hg = H \Rightarrow gg^{-1}Hg = gH \Rightarrow Hg = gH$.

(c) $\Longrightarrow$ (a) Let $g \in G$ and $h \in H$. Then $hg \in Hg$. By (c), $hg \in gH$, so there is some h' in H with $hg = gh'$. Then $g^{-1}hg = h' \in H$. This is true for all choices of g and h, so $H \trianglelefteq G$. $\square$

Lemma (a) If G is Abelian then every subgroup of G is normal in G.

(b) If $H \leqslant G$ and $|G : H| = 2$ then $H \trianglelefteq G$.

Proof (a) If G is Abelian then $g^{-1}hg = hg^{-1}g = h \in H$ for all g in G and all h in H.

(b) If $|G : H| = 2$ then H has two right cosets in G. One of these is H itself, so the other one must be $G \setminus H$. Similarly, the two left cosets of H in G are H and $G \setminus H$. By the previous lemma, $H \trianglelefteq G$. $\square$