13. GROUPS AXIOMS AND PROPERTIES

§13.1. Abstract Groups and the Group Axioms

For Galois, a group was a symmetry group of certain algebraic expressions involving the roots of a polynomial. In time his work was abstracted from its polynomial setting as the emphasis shifted to groups of 'substitutions' (as they were called at the time) or 'permutations' (as we refer to them now). The symbols being permuted could now can be anything, not just roots of polynomials. This was the first stage in the process of abstraction.

A considerable body of theory was built up and many books were written on the subject until around the beginning of this century it was realised that every theorem could be derived from just four simple facts. That resulted in the process of abstraction being continued one stage further as groups and permutations were uncoupled. Now *any* algebraic system which behaves in a manner described by these four axioms could be called a group.

Throughout our mathematical education we've been exposed to a variety of algebraic systems – systems of numbers, systems of vectors, of matrices and of permutations. At any time we generally worked within

one or two of these systems and our objects of study were individual numbers, matrices etc. Now we'll look at algebra through a wide-angle lens. The objects of our consideration will no longer be objects *inside* algebraic systems – they will be the algebraic systems themselves.

'Group' is the name given to a certain type of algebraic structure which satisfies four basic properties called the *group axioms*. On the basis of these axioms it is possible to develop a considerable body of theory – Group Theory. We can prove theorems about groups without needing to know what they are groups of, by basing the proofs solely on these four group axioms.

The advantage of this abstract approach is that we can deal with countless algebraic systems at once. The one theorem in Group Theory immediately becomes a theorem for groups of matrices, and a theorem for groups of numbers, and a theorem for groups of permutations, and so on.

A **binary operation** * on a set G is a function that associates with every ordered pair of elements $a,b \in$ G, a unique element of G, denoted by $a*b$. A **group** (G, $*$) is a set G together with a binary operation $*$ such that:

Closure Law: $a*b \in$ G for all $a, b \in$ G.
Associative Law: $(a * b) * c = a * (b * c)$ for all $a, b, c \in$ G.

Identity Law:There exists $e \in G$ such that $a*e = a = e*a$ for all $a \in G$.

Inverse Law: For all $a \in G$ there exists $b \in G$ such that $a*b = e = b*a$.

COMMENTS

(1) The closure law is really redundant because it's implicit in the definition of a binary operation. However it's usually included for emphasis.

(2) The element e is called the **identity** for G. We show later that it must be unique, that is, a group can only have one identity for its operation.

(3) The element b in the last axiom is called the **inverse** of a (under $*$). It too is unique. Every element has exactly one inverse.

(4) The inverse of the inverse of an element is that element itself.

An **abelian group** G is one which also satisfies the following:

Commutative Law: $a*b = b*a$ for all $a, b \in G$.

§13.2. Examples of Groups

The following two systems are examples of abelian groups:

(1) $(\mathbb{Z}, +)$ is the group of integers under addition. Its identity is 0 and the inverse of an integer n is $-n$.

(2) $(\mathbb{R}^{\#}, \times)$ is the group of all non-zero real numbers under multiplication. Its identity is 1 and the inverse of x is x^{-1}. Note that unlike the first example, the closure law needs a moment's thought in that it requires the observation that $x \neq 0$ and $y \neq 0$ implies $xy \neq 0$.

The next two systems are non-abelian groups:

(3) $(GL(2, \mathbb{R}), \times)$ is the group of all invertible 2 x 2 matrices [matrices with non-zero determinants] with real number entries. Checking the axioms needs a little non-trivial knowledge about matrices. Checking the closure law requires us to know that the product of two invertible matrices is invertible. And we need to know more than the fact that every invertible matrix has an inverse. We need to observe that such an inverse is itself invertible.

(4) $(S_4, \times)$ is the group of all permutations on the set {1, 2, 3, 4}.

The following two algebraic systems are not groups:

(5) $(\mathbb{Z}^{\#}, \times)$ the system of non-zero integers under multiplication is not a group because the Inverse Axiom does not hold. Certainly every non-zero integer *has* an

inverse but in most cases these inverses are not themselves integers. The integer 2, for example, does not have an integer inverse. In fact ±1 are the only ones which have.

(6) If $S = \{x \in \mathbb{R} \mid -10 < x < 10\}$ (i.e. the set of real numbers between −10 and +10) then
(S, +) is not a group because it isn't closed. For example, $5 + 5 \notin S$.

A finite group can be defined by displaying its group table. The set {a, b, c} is a group under the binary operation defined by the table:

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

§13.3. Basic Properties of Groups

Theorem 1: The identity element of a group is unique.
Proof: Suppose e,f are identities for a group $(G,*)$. Then $e = e * f$ (since f is an identity) $= f$ (since e is an identity).


Theorem 2: Each element of a group has only one inverse.
Proof: Suppose b,c are both inverses of the element a in a group $(G, *)$ whose identity is e. Then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. ✋☺

At this stage we'll dispense with the clumsy x, which was only used to avoid confusion with ordinary addition and multiplication of numbers, and to remind ourselves that the operation need not be anything like these arithmetic operations. We use one of two systems of notation when we're discussing groups in general.

Operation	**Multiplicative Notation** Use in general.	**Additive Notation** Use only for abelian groups
Product	ab	$a + b$
Identity	1	0
Inverse of a	a^{-1}	$-a$
Product of n copies of a	a^{n}	na

Theorem 3 (Cancellation Law): If ax = ay then x = y.
Proof: Suppose $ax = ay$. Then $a^{-1}(ax) = a^{-1}(ay)$.
Hence $(a^{-1}a)x = (a^{-1}a)y$. Thus $1x = 1y$ and so $x = y$. ✋☺
[Notice that all the group axioms (except the Closure Law) are needed to prove this.]

Similarly one can prove that $xa = ya$ implies that $x = y$. Thus cancellation on the left or on the right are possible. But beware! We can cancel both sides of an equation on the left and both sides on the right. But we can't cancel one side of the equation by the same factor on the right. So if $ax = ya$ we're not allowed to cancel the a's. Also with expressions such as $y^{-1}xy$ and $x^{-1}y^{-1}xy$ we can't cancel the elements and their inverses unless x and y commute. These expressions play an important role in the theory of non-abelian groups.

A consequence of the Cancellation Law is that for a group every element appears exactly once and only once in the multiplication table.

§13.4. Powers of Elements

Theorem 4: In a group G $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = 1$ and similarly $(ab)(b^{-1}a^{-1}) = 1$. ☺

[Remember that the inverse of a product is the product of the inverses in *reverse* order.]

If g is an element of a group, we define positive integer **powers** of g inductively as follows:

$$g^0 = 1 \; ; \quad g^{n+1} = g^n g \text{ for all } n \geq 0.$$

We define negative powers by $g^{-n} = (g^{-1})^n$ for all negative integers $-n$.

Theorem 5: For all natural numbers m, n and all elements a,b in a group G:

(1) $a^m a^n = a^{m+n}$

(2) $(a^m)^n = a^{mn}$

(3) if G is abelian, $(ab)^n = a^n b^n$

(4) $(b^{-1}ab)^n = b^{-1}a^n b$.

Proof: Although these seem obvious enough (and indeed they are obvious if m,n are positive just by counting factors) the cases where one or both of m,n are negative require special attention.

(1) This is obvious if both m,n are positive or zero. Suppose m is positive and n is negative, say $n = -r$. If $m \geq r$ then on the LHS there will be r cancelling pairs of aa^{-1} leaving $m - r$ $= m + n$, factors of a. If $m < r$ there will be only m such pairs leaving $r - m$ factors of a^{-1}. The result is therefore $a^{-(r-m)} = a^{m-r} = a^{m+n}$.

We've thus proved the result for all n where $m \geq 0$. If m is negative, say $m = -s$, then putting $b = a^{-1}$ the LHS is $b^s b^{-n}$. By the earlier case this is $b^{s-n} = a^{n-s} = a^{m+n}$.

(2) Again this is obvious if m,n are both positive. The other cases are left as exercises.

(3) If n is positive we simply count the number of factors on each side. Because the group is assumed to be abelian here, the factors may be rearranged so all the a's can be

brought to the front. If n is zero, LHS = RHS = 1. If n is negative we put $b = a^{-1}$ and use the positive case.

(4) If n is positive, $(b^{-1}ab)^n = b^{-1}a(bb^{-1})a(bb^{-1})\ ...\ (bb^{-1})ab$ (n factors)

$$= b^{-1}aa\ ...\ ab$$
$$= b^{-1}a^nb.$$

If $n = 0$, LHS = RHS = 1.

If $n = -m$ is negative $(b^{-1}ab)^n = (b^{-1}ab)^{-m}$

$$= ((b^{-1}ab)^{-1})^m$$
$$= (b^{-1}a^{-1}b)^m$$
$$= b^{-1}(a^{-1})^mb$$
$$= b^{-1}a^{-m}b$$
$$= b^{-1}a^nb.$$ ✋☺

§13.5. More Properties of Groups

The **cyclic subgroup generated by** an element g is the set of all powers of g (including 1 as g^0 and negative powers). It is denoted by $\langle \mathbf{g} \rangle$. The **order** of an element g is the smallest positive integer n such that $g^n = 1$. [In additive notation this becomes the smallest positive n such that $ng = 0$.] It is denoted by $|\mathbf{g}|$. If there is no such positive n, we say that g has **infinite order**.

Example 1: In the group of all non-zero complex numbers under multiplication, i has order 4, $\omega = e^{2\pi i/3}$ has order 3, and 2 has infinite order. The identity element of any group is the only element of order 1.

Theorem 6: The order of an element is the order of the cyclic subgroup it generates.
Proof: Suppose g has finite order n. Then $g^n = 1$ but $g^k \neq 1$ if $0 < k < n$. Hence every power of g is g^k for some k with $0 \leq k < n$, and these are distinct since $g^k = g^{k+s}$ for $0 < s < n$ implies that $g^s = 1$, a contradiction. So $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$.
If g has infinite order, ✋☺

Theorem 7: Groups of even order must contain an element of order 2.
Proof: Suppose |G| is even. Now the elements of G which differ from their inverses must come in pairs $\{x, x^{-1}\}$. Since |G| is even, the remaining elements, those for which $x = x^{-1}$, must also be even in number. Now $x = x^{-1}$ is equivalent to $x^2 = 1$ and so these are the elements of order 2, together with the identity. Leaving out the identity, there must be an odd number of elements of order 2 and so the number of elements of order 2 must be at least 1. ✋☺

Theorem 8: If all of the elements of G (except 1) have order 2, then G must be abelian.
Proof: Let $x, y \in$ G. Then $(xy)^2 = 1$. But also $x^2y^2 = 1$ and so $xyxy = xxyy$.
Multiplying by x^{-1} on the left and by y^{-1} on the right of each side of the equation we conclude that $yx = xy$. Since this holds for all $x, y \in$ G it follows that G is abelian. ✋☺

§13.6. Cyclic Groups

A group G is **cyclic** if it can be generated by a single element, that is if $G = \langle g \rangle$ for some $g \in G$. It is called the **cyclic group generated by** g.)

Example 2: The set of n-th roots of unity, $G = \{z \in \mathbb{C} \mid z^n = 1\}$, is a group under multiplication. It is a cyclic group because it can be generated by $e^{2\pi i/n}$. This is because every n^{th} root of 1 has the form $e^{2\pi ki/n} = (e^{2\pi i/n})^k$.
In particular the group of 4^{th} roots of unity is $\{1, i, -1, -i\}$ which is generated by i.

Example 3: The group of symmetries of a parallelogram is {I, R} where R is a 180° rotation about its centre. This group is thus generated by R.

Example 4: The group $(\mathbb{Z},+)$ of integers under addition is cyclic because it can be generated by the integer 1. Remember that we're using additive notation here so instead of saying that every integer is an integer power of 1 (which is not the case), we should be saying that every integer is an integer multiple of 1 (which it is). Note that −1 also generates this group, but ±1 are the only generators.

Theorem 9: Cyclic groups are abelian.
Proof: Two typical elements in the cyclic group $\langle g \rangle$ are g^r and g^s. Now $g^r g^s = g^{r+s} = g^s g^r$. So every pair of elements commute and hence the cyclic group is abelian. ✋☺

Theorem 10: A finite group of order n is cyclic if and only if it contains an element of order n.
Proof: If $|G| = n$ and G has an element g of order n then $\langle g \rangle$, the cyclic subgroup generated by g has order n. Thus there are no other elements in G. They are all powers of g and so g is a generator for G and hence G is cyclic.

Conversely suppose that G is a cyclic group of order n. Then if g is a generator, g must have order n. ✋☺

Example 5: The group given by the following multiplication table is not cyclic since it has no element of order 4.

	A	**B**	**C**	**D**
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

SUMMARY

Group Axioms: Closure, **Associative:** $(xy)z = x(yz)$, **Identity:** 1, **Inverses:** g^{-1}.

Abelian Group: Group + **Commutative:** $xy = yx$].

Uniqueness: The identity and inverses are unique.

Cancellation: You can cancel by any element if it is on the same end of LHS and RHS

Group Table: ab is in row a and column b (For convenience put 1 first.)

Every element appears exactly once in every row and column.

Elements of order 2 show up by having 1 on the diagonal.

A group is abelian if its group table is symmetric.

Powers: Defined as for numbers ($g^0 = 1$).

Usual basic index laws hold except that $(ab)^n = a^n b^n$ only holds if $ab = ba$ (a, b commute).

Note that $(b^{-1}ab)^n = b^{-1}a^n b$ and $(ab)^{-1} = b^{-1}a^{-1}$ hold in any group.

Cyclic Subgroups: $\langle g \rangle$ = the set of all powers of g.

Order of Element: $|g|$ = smallest positive power n such that $g^n = 1$.

Order of Group: |G| = number of elements in G.

Note: $|g| = |\langle g \rangle|$.

Elements of Order 2: Groups of even order contain an element of order 2.

Groups in which every element has order 2 must be abelian.

Cyclic Groups: G is cyclic if $G = \langle g \rangle$ for some generator g. Cyclic groups are abelian.
If $|G| = n$, G is cyclic if and only if it has an element of order n.

EXERCISES FOR CHAPTER 13

Exercise 1: Which of the following algebraic systems, G, are groups? In each case where G is not a group state which group axioms fail. In each case where G is a group answer the following questions find the identity of G, the inverse of a typical element and state whether G is abelian or cyclic?

(a) The set of real numbers under addition.
(b) The set of real numbers under subtraction.
(c) The set of positive real numbers under multiplication.
(d) The set of all 2×2 real invertible matrices under matrix multiplication.
(e) The set of all 2×2 real invertible matrices under matrix addition.
(f) The set of complex numbers whose modulus is 1, under multiplication.
(g) The set of all complex cube roots of unity under multiplication.
(h) The set {0, 1, 2, 3, 4, 5} under addition modulo 6.
(i) The set {1, 2, 3, 4, 5} under multiplication modulo 6.
(j) The set of all real numbers of the form 2^n where n is an integer.

(k) The set of all vectors in $\mathbb{R}^3$ under the cross product.
(l) The set of functions {f, g, h, k} where f(x) = x; g(x) = $-x$; h(x) = x^{-1}; k(x) = $-x^{-1}$ under the operation of composition of functions (function of a function).

Exercise 2: Let G = {x ∈ ℝ | x ≠ −1} denote the set of real numbers excluding −1, and let the binary operation ∗ be defined on G by: a∗b = a + b + ab

(i) Prove that (G, ∗) is a group.

(ii) What is the inverse of 2?

(iii) How many elements does G have of order 2?

Exercise 3: Prove that the set of all real 2×2 matrices $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is a group under matrix multiplication.

Exercise 4: Find all possible group tables for groups of order 1, 2 or 3.

Exercise 5: Find the numbers of elements of each order in the following two groups whose group tables are given:

(a)

	1	**a**	**b**	**c**
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

(b)

	1	**a**	**b**	**c**
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

Exercise 6: Find the orders of the elements in the cyclic group of order 6.

Exercise 7: Find the orders of the elements of the following three groups:
G = the group {0, 1, 2, 3, 4, 5, 6, 7} under addition 8;
H = the group {1, 3, 7, 9, 11, 13, 17, 19} under multiplication modulo 20;
K = the dihedral group of order 8.
Show that no two of these groups are isomorphic.

Exercise 8: Which of the above three groups of order 8 is cyclic? Which are abelian?

Exercise 9: Find $\langle 9 \rangle$, the cyclic group generated by 9, in the group $\mathbb{Z}_{100}^{\#}$. This consists of all the integers from 1 to 99 which have no factors in common with 100. The operation is multiplication modulo 100. Also determine the order of 9 in this group.

Exercise 10: Find the order of the following elements in the group $\mathbb{Z}_{100}$ (consisting of all the integers from 0 to 99 under addition modulo 100):

2, 9, 6, 15.

Exercise 11: Which of the following algebraic systems, G, are groups? In each case where G is not a group state which group axioms fail. In each case where G is a group answer the following questions: Find the identity of G, the inverse of a typical element and state whether G is abelian or cyclic?

(a) The set of even integers under addition.

(b) The set of even integers under multiplication.

(c) The set $\{\pm 1, \pm i\}$ under multiplication.

(d) The set of all 2×2 real symmetric matrices under matrix multiplication.

(e) The set of all 2×2 matrices of the form:

$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ where a,b are both non-zero, under matrix multiplication.

(f) The set of complex numbers whose argument is an integer multiple of $\pi/4$, under multiplication.

(g) The set of all complex numbers z such that z^3 is real, under multiplication.

(h) The set {0, 1, 2, 3, 4, 5, 6} under addition modulo 7.

(i) The set {1, 2, 3, 4, 5, 6} under multiplication mod 7.

(j) The set of all complex numbers z such that z^n is real for some integer n, under multiplication.

(k) The set of all non-zero real numbers of the form

$$a + b\sqrt{2},$$

where a, b are rational numbers, under multiplication.
(l) The set of subsets of {1, 2, 3, 4} under the operation: $S * T = S \cup T - (S \cap T)$.

Exercise 12: Let $G = \{z \in \mathbf{C} \mid z \neq 1\}$ denote the set of real numbers excluding 1, and let the binary operation $*$ be defined on G by: $a*b = ab - a - b + 2$

(i) Prove that $(G, *)$ is a group.

(ii) What is the inverse of i?

(iii) How many elements does G have of order 3?

Exercise 13: Prove that the set of all real 2×2 matrices of the form $\begin{pmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{pmatrix}$ is a group under matrix multiplication.

Exercise 14: Find all the possible ways of completing the following group table:

	1	**a**	**b**	**c**
1				
a				
b				
c				

Which of these groups are isomorphic?

Exercise 15: Complete the following group table and find the numbers of elements of each order.

	1	**a**	**b**	**c**	**d**	**e**
1						
a		1	c	b		d
b			d	a	1	
c		d	e		a	b
d		c		e	b	a
e		b	a		c	1

Exercise 16: Find the orders of the elements of the following three groups:

$$G = \{1, \quad -1, \quad i, \quad -i, \quad \frac{1+i}{\sqrt{2}}, \quad \frac{1-i}{\sqrt{2}}, \quad \frac{-1+i}{\sqrt{2}}, \quad \frac{-1-i}{\sqrt{2}}\}$$

under multiplication;
H = the group of symmetries of a rectangular box;
K = the group of order 8 whose group table is:

	1	**–1**	**i**	**–i**	**j**	**–j**	**k**	**–k**
1	1	–1	i	–i	j	–j	k	–k
–1	–1	1	–i	i	–j	j	–k	k
i	i	–i	–1	1	k	–k	–j	j
–i	–i	i	1	–1	–k	k	j	–j
j	j	–j	–k	k	–1	1	i	–i
–j	–j	j	k	–k	1	–1	–i	i
k	k	–k	j	–j	i	–i	–1	1
–k	–k	k	–j	j	–i	i	1	–1

Show that no two of these groups are isomorphic.

Exercise 17: Find the numbers of elements of each order in the cyclic group of order 12.

Exercise 18: Which of the above three groups of order 8 is cyclic? Which are abelian?

Exercise 19: Find the order of the following elements in the group $\mathbb{Z}_{17}^{\#}$ (consisting of all the integers from 1 to 16 under multiplication modulo 17):

2, 6, 9, 15.

SOLUTIONS FOR CHAPTER 13

Exercise 1:

(a) G is a group. The identity is 0. The inverse of x is $-x$. G is abelian but not cyclic. [Clearly 0 is not a generator, and a non-zero number x can never generate x/2 under addition and so can't be a generator.]

(b) G is not a group. The system is certainly closed but subtraction is not associative.

$[(x - y) - z = x - y - z$ while $x - (y - z) = x - y + z.]$

Nor is there an identity. Sure, $x - 0 = x$ for all x, but an identity has to work on *both* sides and $0 - x = x$ is only true for $x = 0$. Since there's no identity there can't be inverses.

(c) This is a group. The identity is 1 and the inverse of x is $1/x$. This group is abelian but not cyclic. [If x was a generator then x^n would have to equal 1 for some integer n. However the only real n'th root of unity is 1 itself and clearly doesn't generate the group.]

(d) This is a group. [The product of two matrices with inverses is also invertible: $(AB)^{-1} = B^{-1}A^{-1}$. Matrix multiplication is associative.] The identity is the 2×2 identity matrix I and the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ This group is non-abelian (and so can't possibly be cyclic).

(e) This is not a group. For a start, it isn't closed [I and –I are invertible but not their sum, the zero matrix]. Nor is there an identity [the zero matrix is the only possibility, but as we have just pointed out it's not in the system. All this system has going for it is that the operation *is* associative. And even though it's true that (–A) is invertible if A is invertible, we can't claim that inverses exist if the system doesn't have an identity.

(f) This is a group. If $|a| = 1$ and $|b| = 1$ then $|ab| = 1$ and so G is closed. Multiplication of complex numbers is associative. The identity is 1 and the inverse of z is 1/z. [Note it is not enough to observe that if $|z| = 1$, 1/z exists. We must note that $|1/z| = 1/|z| = 1$ thus checking that 1/z

belongs to the system.] This group is abelian but is not cyclic [If g is a generator then, since $-1 \in G$, $g^n = -1$ for some integer $n > 0$. But then $g^{2n} = 1$ and so g would only have n distinct powers while G is infinite.]

(g) $G = \{1, \omega, \omega^2\}$ and so is clearly a cyclic (and hence abelian) group of order 3.

(h) This is a cyclic (and hence, abelian) group. The identity is 0, the inverse of x is $6 - x$. The generators are 1 and 5.

(i) This is not a group. It is closed, the operation is associative and 1 is the identity. It falls down at the last axiom. Some elements do not have inverse. In fact 1 and 5 are the only ones which do. [For what x is $2x = 1 \pmod 6$? None, of course!]

(j) This is a cyclic (and hence, abelian) group. The identity is $1 = 2^0$, the inverse of 2^n is 2^{-n}. The generators are 2 and ½.

(k) This is not a group since the cross product of vectors is not associative.

(l) This is a group of order 4, containing 3 elements of order 2, plus the identity function f. [For example g has order 2 since $g(g(x)) = -(-x) = x = f(x)$ so $g^2 = f$.] Since G has no element of order 4, it can't be cyclic.

Exercise 2: This is a very good example on which to practice ones skills in *Proof By Contradiction*.

Closure: Let $a, b \in$ G, so $a \neq -1$ and $b \neq -1$. Suppose $a*$b $= -1$. Then $a + b + ab = -1$ and so $(a + 1)(b + 1) = 0$ which implies that $a = -1$ or $b = -1$, a contradiction.

Associative: Unlike the examples in exercise 1, this is a totally new operation that we have never encountered before. We must therefore carefully check the associative law.

$(a*b)*c = (a*b) + c + (a*b)$c

$= ab + a + b + c + (ab + a + b)c$

$= a + b + c + ab + ac + bc + abc$

Similarly a$*(b*c)$ has the same value (we can actually see this by the symmetry of the expression.

Identity: An identity, e, would have to satisfy: $e*x = x = x*e$ for all $x \in$ G, that is, $ex + e + x = x$, or $e(x + 1) = 0$ for all x. Clearly $e = 0$ works. The identity is 0.

Inverses: If $x*y = 0$, then $xy + x + y = 0$. So $y(x + 1) = -x$ and hence $y = -x/(x + 1)$. This exists for all $x \neq -1$, i.e. for all $x \in$ G. But we must also check that it is itself an element of G. Suppose $-x/(x + 1) = -1$. Then $-x = -x - 1$, which gives $0 = -1$. This is clearly a contradiction and hence y must be in G.

Exercise 3:

Closure: $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$

$= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ \cos\alpha\sin\beta + \sin\alpha\cos\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{pmatrix}$

$= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}$

Associative: The operation is matrix multiplication and so is associative.

Identity: The identity is the identity matrix $= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix}$ which has the required form.

Inverses: The determinant of $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is $\cos^2\theta + \sin^2\theta = 1$ and so the inverse is $\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \cos(-\theta) & \sin(-\theta) \\ -\sin(-\theta) & \cos(-\theta) \end{pmatrix}$ which is in the system.

Exercise 4:

Order 1: If there is only one element in a group, it must be the identity and so the group table is simply:

	1
1	1

Order 2: A group of order 2 has two elements 1, *x*. Filling out the table using the property of 1 we get:

	1	**x**
1	1	x
x	x	

Since every element appears exactly once in every row and column, the missing entry must be 1 and so the complete table is:

	1	**x**
1	1	x
x	x	1

Order 3: Denoting the elements by 1, *x*, *y* we get:

	1	**x**	**y**
1	1	x	y
x	x		?
y	y		

Now *xy* can't be *x* (as its already in that row) and it can't be *y* (as its already in that column) so it must be 1. The table can now be completed using the same principle:

	1	**x**	**y**
1	1	x	y
x	x	y	1
y	y	1	x

Thus we've shown that there is only one group for each of the orders 1, 2 and 3.

Exercise 5:
(a) has the 1 plus 3 elements of order 2.
(b) has 1, one element of order 2 (viz. b) and 2 elements of order 4.
[The fact that they differ in their structure in this way means that they are non-isomorphic, or essentially different. These two tables reflect the only two possible group structures for a group of order 4.]

Exercise 6: The cyclic group of order 6 has the form:

$$\{1, g, g^3, g^3, g^4, g^5\} \text{ where } g^6 = 1$$

Clearly g has order 6.
$(g^2)^2 = g^4$, $(g^2)^3 = g^6 = 1$ and so g^2 has order 3.
$(g^3)^2 = 1$ and so g^3 has order 2.
$(g^4)^2 = g^8 = g^2$, $(g^4)^3 = g^{12} = 1$ and so g^4 has order 3;
Finally, $g^5 = g^{-1}$ and so clearly has order 6.
The cyclic group of order 6 thus has:
1 element of order 1;
1 element of order 2;
2 elements of order 3;
2 elements of order 6.
NOTE: orders 4 and 5 are missed out as possible orders. Can you guess why?

Exercise 7:
G: 1, 3, 5, 7 have order 8
2, 6 have order 4
4 has order 2
0 has order 1

H: 3, 7, 13 and 17 have order 4
9, 11 and 19 have order 2
1 has order 1

K: The dihedral group
$\langle a, b \mid a^4 = b^2 = 1, ab = ba^{-1} \rangle$ has elements 1, a, a^2, a^3, b, ab, a^2b, a^3b. Of these:
a, a^3 have order 4
a^2, b, ab, a^2b, a^3b have order 2;
1 has order 1.

NOTE: The order of the group is a power of 2 and the orders of the elements are likewise powers of 2. This is quite significant.

Listing the numbers of the elements of orders 1, 2, 4 and 8 as vectors we have:
G: (1, 1, 2, 4); H: (1, 3, 4, 0); K: (1, 5, 2, 0)
The differences show that these three groups are mutually non-isomorphic. There are in fact 5 distinct groups of order 8, the above three plus two others.

Exercise 8: G is cyclic (and hence abelian) because it contains an element of order 8; H is abelian but not cyclic; K is non-abelian (and hence not cyclic).

NOTE: There's always only one cyclic group of any given order. In other words, all cyclic groups of order n are isomorphic to0 one another. A representative example of the cyclic group of order n is $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ of integers modulo n under addition.

Exercise 9: The powers of 9 are $9^1 = 9$, $9^2 = 81$, $9^3 = 729 = 29 \bmod 100$ and so on.
Rather than accumulate the higher and higher powers we can simply multiply by 9 at each stage to get the next, for example, $9^4 = 9 \times 29 = 261 = 61 \bmod 100$. Then come 49, 41, 69, 21, 89 and finally 1.
So $\langle 9 \rangle = \{1, 9, 81, 29, 61, 49, 41, 69, 21, 89\}$. There are 10 elements in this cyclic subgroup and so 9 has order 10 under multiplication modulo 100.

Exercise 10:
2: Remember that the operation is addition, so we need to keep adding the generator to itself, that is, taking higher and higher multiples, not powers. We want the smallest positive integer n such that $2n \equiv 0 \bmod 100$, or in other words, such that $2n$ is a multiple of 100. The answer is clearly 50.
9: We want 100 to divide $9n$. Since 100 has no factors in common with 9, we'd need n itself to be a multiple of 100. The smallest positive such n is thus 100. So 9 has order 100 in this group.
6: We need $6n$ to be a multiple of 100. Since 2 divides both 6 and 100 we need 50 to divide $3n$. But since 50 has no factor in common with 3, we'd need 50 to divide n. So 6 has order 50.
15: $15n \equiv 0 \bmod 100$ means $3n = 0 \bmod 20$. Since 3 is coprime with 20, we need $n = 0 \bmod 20$, so 15 has order 20.