THE UNIVERSITY OF SYDNEY

MATH2008 Introduction to Modern Algebra

(http://www.maths.usyd.edu.au/u/UG/IM/MATH2008/)

Semester2, 2003 Lecturer: R. Howlett

Tutorial 5

1. For each of the following operations, determine whether or not the set $\mathbb{Z}$ of integers is a group under the operation: addition, subtraction, multiplication, division.

Solution.

Remember that an operation on a set S is, by definition, a rule that takes pairs of elements of S as input, and yields an element of S as output. The question asserts that addition, subtraction, multiplication and division are operations on $\mathbb{Z}$, but this is something that ought to be checked. In fact, division is not an operation on $\mathbb{Z}$: for one thing, x/y is not defined for all pairs of integers x and y—specifically, it is not defined when y is zero—and, for another, the result of dividing an integer by an integer is not necessarily an integer.

Since division does not even determine an operation on $\mathbb{Z}$, it is certainly not true that $\mathbb{Z}$ is a group under division.

It is true that $\mathbb{Z}$ is a group under addition. The associative law is satisfied ($(x+y)+z = x+(y+z)$ for all x, y, $z \in \mathbb{Z}$), and the number 0 satisfies the requirements of the second axiom: $x+0 = 0+x = x$ for all $x \in \mathbb{Z}$, and for all $x \in \mathbb{Z}$ there is a $y \in \mathbb{Z}$ (namely, $y = -x$) such that $x+y = y+x = 0$.

It is not true that $\mathbb{Z}$ is a group under subtraction, since the associative law does not hold for subtraction. For example, $3-(2-1) = 2$ but $(3-2)-1 = 0$.

It is not true that $\mathbb{Z}$ is a group under multiplication. The number 1 is an identity element for this operation, and it is the only identity element since (as was proved in lectures) an operation can have at most one identity element. But now the second part of the second axiom is not satisfied: it is not true that for all $x \in \mathbb{Z}$ there is a $y \in \mathbb{Z}$ such that $xy = 1$. This can be proved by taking $x = 2$: there is no $y \in \mathbb{Z}$ such that $2y = 1$ (since $\frac{1}{2} \notin \mathbb{Z}$).

2. Check that the set $\mathbb{C}\backslash\{0\}$ (the set of all nonzero complex numbers) is a group under multiplication of complex numbers (defined in the usual way).

Solution.

The properties of complex numbers that are needed here should be familiar from junior level maths. However, we shall write out proofs based on the even more familiar properties of real numbers.

Every complex number can be uniquely expressed in the form $a+bi$, where a and b are real numbers, i being a fixed square root of -1. Multiplication of

complex numbers is given by the formula

$$(a+bi)(c+di) = (ac-bd)+(ad+bc)i \qquad (1)$$

for all a, b, c, $d \in \mathbb{R}$. This unambiguously defines $\alpha\beta$ for all α, $\beta \in \mathbb{C}$, since we can uniquely write α as $a+bi$ and β as $c+di$. For this question, we need to show that it defines an operation on $\mathbb{C}\backslash\{0\}$. In other words, we need to show that if α and β are arbitrary nonzero complex numbers then $\alpha\beta$ is defined and is a nonzero complex number. Since Eq. (1) above defines $\alpha\beta$ as a complex number, we need to prove that it is nonzero. However, we shall prove some other things first.

We start by proving that multiplication of complex numbers is associative. Let α, β and γ be arbitrary complex numbers. Then we have $\alpha = p+qi$, $\beta = r+si$ and $\gamma = t+ui$ for some p, q, r, s, t, $u \in \mathbb{R}$, and (1) gives

$$\begin{aligned}
\alpha(\beta\gamma) &= (p+qi)((r+si)(t+ui)) \\
&= (p+qi)((rt-su)+(ru+st)i) \\
&= (p(rt-su)-q(ru+st))+(p(ru+st)+q(rt-su))i \\
&= (prt-psu-qru-qst)+(pru+pst+qrt-qsu)i \\
&= ((pr-qs)t-(ps+qr)u)+((pr-qs)u+(ps+qr)t)i \\
&= ((pr-qs)+(ps+qr)i)(t+ui) \\
&= ((p+qi)(r+si))(t+ui) = (\alpha\beta)\gamma.
\end{aligned}$$

Hence the associative law is satisfied.

Next, observe that $1 = 1+0i$ is an identity element for complex multiplication: if we put $a = 1$ and $b = 0$ in (1) then the right hand side becomes $(1c-0d)+(1d+0c)i = c+di$, showing that $1\beta = \beta$ for all $\beta \in \mathbb{C}$, and similarly putting $c = 1$ and $d = 0$ in (1) shows that $\alpha 1 = \alpha$ for all $\alpha \in \mathbb{C}$.

If $\alpha \in \mathbb{C}\backslash\{0\}$ then $\alpha = a+bi$ for some a, $b \in \mathbb{R}$ that are not both zero. Then $a^2+b^2 > 0$, and we may define $c+di \in \mathbb{C}$ by $c = \frac{a}{a^2+b^2}$ and $d = \frac{-b}{a^2+b^2}$. This gives $ac-bd = \frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2} = 1$, and $ad+bc = \frac{-ab}{(a^2+b^2} + \frac{ba}{a^2+b^2} = 0$, so that Eq. (1) gives $(a+bi)(c+di) = 1$. Similarly, $(c+di)(a+bi) = 1$, and so we have shown that for each $\alpha \in \mathbb{C}\backslash\{0\}$ there is an α^{-1} such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$.

Finally, we show that the product of two nonzero complex numbers is nonzero. Let α, $\beta \in \mathbb{C}\backslash\{0\}$, and suppose (for a contradiction) that $\alpha\beta = 0$. Since $\alpha \neq 0$ and $\beta \neq 0$, there exist α^{-1}, $\beta^{-1} \in \mathbb{C}$ with $\alpha^{-1}\alpha = 1$ and $\beta\beta^{-1} = 1$. Since the right hand side of (1) is zero if $a = b = 0$ or if $c = d = 0$, we know that $\gamma\delta = 0$ if $\gamma = 0$ or if $\delta = 0$. Now since $\alpha\beta = 0$ by hypothesis, we have

$$0 = \alpha^{-1}0 = \alpha^{-1}(0\beta^{-1}) = \alpha^{-1}((\alpha\beta)\beta^{-1}) = \alpha^{-1}(\alpha(\beta\beta^{-1})) = (\alpha^{-1}\alpha)(\beta\beta^{-1}),$$

by two applications of the associative law. Since this immediately gives $0 = 1$, we have obtained the desired contradiction.

This last paragraph shows that multiplication does define an operation on $\mathbb{C}\backslash\{0\}$. The preceding calculations showed that it is associative and has an identity element, and that each element of $\mathbb{C}\backslash\{0\}$ has an inverse with respect to this operation. Hence $\mathbb{C}\backslash\{0\}$ is a group under the operation.

3. Consider a fixed row in the multiplication table of a group G. The row contains all the products ax, where a is fixed and x varies.

(i) Show that no element occurs twice in the row. (*Hint*: if an element occurred twice it would mean that $ax = ay$ for some x and y with $x \neq y$. Multiply both sides of this equation by a^{-1}.)

(ii) Show that every element of G occurs in the row. (*Hint*: to show that b occurs you must find an x such that $ax = b$; you should be able to find a suitable formula for x in terms of a and b.)

(iii) Redo This question replacing "row" by "column".

Solution.

(i) Suppose that b occurs twice in the row that contains all the products ax, where x runs through the elements of G. Then there exist two distinct elements $x, y \in G$ with $ax = ay = b$. But now

$$x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = ey = y,$$

contradicting $x \neq y$.

(ii) Let $b \in G$ be arbitrary, and put $x = a^{-1}b$. Then

$$ax = a(a^{-1}b) = (aa^{-1})b = eb = b,$$

showing that b occurs in the row corresponding to a.

(iii) Since $b = be = b(a^{-1}a) = (ba^{-1})a$, we see that b occurs in the column corresponding to a. If it occurred twice we would have $xa = ya = b$ for some x, $y \in G$ with $x \neq y$, but then

$$x = xe = x(aa^{-1}) = (xa)a^{-1} = (ya)a^{-1} = y(aa^{-1}) = ye = y,$$

giving a contradiction.

4. Suppose that the vertices of an equilateral triangle lie at points labelled 1, 2 and 3 (anticlockwise). Let ρ be the symmetry given by an anticlockwise rotation of the triangle through 120°, and let ρ' similarly be given by a clockwise rotation through 120°. For each $i \in \{1, 2, 3\}$, let σ_i be the reflection in the line through the point labelled i perpendicular to the line joining the other two points.

(i) Determine the permutations associated with each of the symmetries of the triangle.

(ii) Write out the full multiplication table for the group of symmetries of the triangle. (List the symmetries in the following order: e (= identity), ρ, ρ', σ_1, σ_2, σ_3.)

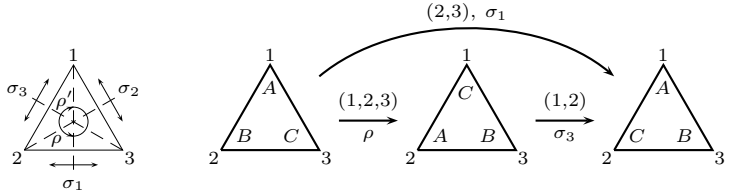
(iii) Check that the composite of the symmetry associated with the permutation $(1, 2, 3)$ followed by the symmetry associated with $(1, 2)$ is the symmetry associated with $(1, 2, 3)(1, 2) = (2, 3)$. (You may find it useful to label the vertices of the triangle A, B and C. The symmetries move A, B and C but leave the locations 1, 2 and 3 fixed.)

Solution.

The identity symmetry corresponds to id, the identity permutation; ρ corresponds to $(1, 2, 3)$ and ρ' to $(1, 3, 2)$, and σ_1, σ_2, σ_3 to $(2, 3)$, $(1, 3)$, $(1, 2)$ respectively. The multiplication table is as follows:

	e	ρ	ρ'	σ_1	σ_2	σ_3
e	e	ρ	ρ'	σ_1	σ_2	σ_3
ρ	ρ	ρ'	e	σ_2	σ_3	σ_1
ρ'	ρ'	e	ρ	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	e	ρ'	ρ
σ_2	σ_2	σ_1	σ_3	ρ	e	ρ'
σ_3	σ_3	σ_2	σ_1	ρ'	ρ	e

The diagram shows that the composite of ρ followed by σ_3 equals σ_1—as it should, since $1 \overset{(1,2,3)}{\longmapsto} 2 \overset{(1,2)}{\longmapsto} 1 = 1^{(2,3)}$, $2 \overset{(1,2,3)}{\longmapsto} 3 \overset{(1,2)}{\longmapsto} 3 = 2^{(2,3)}$ and $3 \overset{(1,2,3)}{\longmapsto} 1 \overset{(1,2)}{\longmapsto} 2 = 3^{(2,3)}$. All entries of the table can be checked similarly.



5. For each element a of the group of symmetries of an equilateral triangle, find the smallest positive integer n such that $a^n = e$.

Solution.

In any group, the *order* of an element a is defined to be the least positive integer n such that a^n is the identity (or infinity if there is no such integer). From the table we see that $\rho^2 = \rho'$, and $\rho^3 = \rho\rho' = e$. Hence ρ has order 3. The other orders are found similarly:

Element	e	ρ	ρ'	σ_1	σ_2	σ_3
Order	1	3	3	2	2	2

6. Let S be the set $\{2, 4, 6, 8\}$. Define an operation $*$ on S as follows: for all a, $b \in S$, let $a * b$ be the final digit in the standard base 10 notation for the product ab. (Thus, $8 * 8 = 4$, since $8 \times 8 = 64$.) Write out the multiplication table for $*$, and determine whether or not S is a group under this operation.

Solution.

This operation does make S into a group. The multiplication table is the same as for the group of complex numbers $\{1, i, -1, -i\}$ under multiplication. The elements of the group can be written as x^0 = identity, x, x^2, x^3, where x^4 = identity. In this example we can take $x = 2$; the identity is 6. Groups with this structure are said to be *cyclic of order 4*.

$*$	6	2	4	8
6	6	2	4	8
2	2	4	8	6
4	4	8	6	2
8	8	6	2	4