

Tutorial 2

1. Let G be a group and S a set on which a multiplication operation is defined. Let $\phi: G \rightarrow S$ be a function that satisfies $(\phi x)(\phi y) = \phi(xy)$ for all $x, y \in G$. Prove that the image of ϕ is a group, with multiplication compatible with multiplication in S .

Solution.

We must first show that $\text{im } \phi$ has a multiplication operation that is “compatible with multiplication in S ”. That is, we need there to be a function $\text{im } \phi \times \text{im } \phi \rightarrow \text{im } \phi$ such that each pair $(s, t) \in \text{im } \phi \times \text{im } \phi$ maps to st , the product of s and t considered as elements of S . For this we simply need $st \in \text{im } \phi$ whenever $s, t \in \text{im } \phi$. Now if $s, t \in \text{im } \phi$ then $s = \phi g$ and $t = \phi h$ for some $g, h \in G$, and in view of our assumption that ϕ preserves multiplication, this gives

$$st = (\phi g)(\phi h) = \phi(gh),$$

which is in $\text{im } \phi$, as required.

Now we must check the axioms. Let $r, s, t \in \text{im } \phi$. Then there exist $a, b, c \in G$ with $r = \phi a$, $s = \phi b$ and $t = \phi c$. It follows that

$$(rs)t = ((\phi a)(\phi b))(\phi c) = (\phi(ab))(\phi c) = \phi((ab)c)$$

and

$$r(st) = (\phi a)((\phi b)(\phi c)) = (\phi a)(\phi(bc)) = \phi(a(bc)).$$

But G is a group; so $a(bc) = (ab)c$, and so $(rs)t = r(st)$. Since r, s and t are arbitrary elements of $\text{im } \phi$ we conclude that the associative law holds in $\text{im } \phi$.

We must show that there exists an element $e \in \text{im } \phi$ such that for all $r \in \text{im } \phi$,

- (a) $er = re = r$,
 (b) there exists $s \in \text{im } \phi$ with $rs = sr = e$.

Define $e = \phi 1$, where 1 is the identity element of G , and let $r \in \text{im } \phi$. Then $r = \phi g$ for some $g \in G$. Put $s = \phi(g^{-1})$. Then

$$er = (\phi 1)(\phi g) = \phi(1g) = \phi g = r = \phi g = \phi(g1) = (\phi g)(\phi 1) = re$$

and

$$rs = (\phi g)(\phi g^{-1}) = \phi(gg^{-1}) = \phi 1 = e = \phi 1 = \phi(g^{-1}g) = (\phi g^{-1})(\phi g) = sr$$

as required.

2. Let S be a set with a multiplication operation. An element $e \in S$ is called a *left identity* if $es = s$ for all $s \in S$, and an element $f \in S$ is called a *right identity* if $sf = s$ for all $s \in S$.

- (i) Prove that if S contains both a left identity and a right identity then they are equal.
 (ii) Find an example of an S that contains a left identity but no right identity. (Hint: use 2×2 matrices.)

Solution.

- (i) Let e be a left identity in S and f a right identity in S . Then

$$ex = x \quad \text{for all } x \in S, \tag{1}$$

and

$$yf = y \quad \text{for all } y \in S. \tag{2}$$

Putting $x = f$ in Eq. (1) gives $ef = f$, while putting $y = e$ in Eq. (2) gives $ef = e$. Hence $e = f$, as required.

- (ii) Let S be the set of all 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, where a, b are integers. With matrix multiplication defined as usual, we find that for all integers a, b, a', b' we have

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} aa' & ab' \\ 0 & 0 \end{pmatrix} \in S,$$

and so matrix multiplication yields a multiplication operation on S . Now let $E \in S$ be the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Since

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

for all integers a, b , it follows that E is a left identity element for S . However, it is not true that $AE = A$ for all $A \in S$, since, for example,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

So E is not an identity element in S .

3. Let R be a ring and define $R^n = \{(x_1, x_2, \dots, x_n) \mid x_i \in R\}$, where n is a fixed positive integer. Define addition and multiplication on R^n by the rules

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n),$$

$$(x_1, x_2, \dots, x_n)(y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

Is it true, for all R and n , that R^n is a ring under these operations?

Solution.

The answer is “yes”. The *direct product*, of two rings R and S , is the set T given by $T = \{(r, s) \mid r \in R, s \in S\}$, with addition and multiplication defined componentwise. Proving that the axioms hold in T is straightforward, using in each case that the axiom in question is satisfied in R and in S . By way of illustration, the proof for one of the distributive laws is written out below. Exactly the same methods work for the direct sum of 3 or more rings. In particular, the direct sum of n copies of any ring R is also a ring.

The Left Distributive Law says that $t_1(t_2 + t_3) = t_1 t_2 + t_1 t_3$ for all t_1, t_2 and t_3 . To show that this holds in T (as defined above), let t_1, t_2, t_3 be arbitrary elements of T . Then there exist $r_1, r_2, r_3 \in R$ and $s_1, s_2, s_3 \in S$ such that $t_i = (r_i, s_i)$ for each i , and now

$$\begin{aligned} t_1(t_2 + t_3) &= (r_1, s_1)((r_2, s_2) + (r_3, s_3)) = (r_1, s_1)(r_2 + r_3, s_2 + s_3) \\ &= (r_1(r_2 + r_3), s_1(s_2 + s_3)) = (r_1 r_2 + r_1 r_3, s_1 s_2 + s_1 s_3) \\ &\quad \text{(by distributivity in } R \text{ and } S) \\ &= (r_1 r_2, s_1 s_2) + (r_1 r_3, s_1 s_3) = (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3) = t_1 t_2 + t_1 t_3, \end{aligned}$$

as required.

4. Let R be a ring with the property that $a^2 = a$ for all $a \in R$. Prove that $a + a = 0$ for all $a \in R$, and that R is commutative. Show also that R , with its given addition operation, can be made into a vector space over the field of two elements.

Solution.

For all $a \in R$,

$$a + a = (a + a)(a + a) = a^2 + a^2 + a^2 + a^2 = a + a + a + a.$$

Adding $-a - a$ to both sides gives $a + a = 0$.

For all $a, b \in R$,

$$a + b = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b.$$

Since $a + a = b + b = ab + ab = 0$, adding a, b and ab to both sides gives $ab = ba$.

Let $F = \{0_F, 1_F\}$ be the two-element field. We need to define scalar multiplication $\mathbb{F}_2 \times R \rightarrow R$ so that the vector space axioms hold. It is clear that we must define $0_F a = 0$ and $1_F a = a$ for all $a \in R$, and we need only check that $\lambda(\mu a) = (\lambda\mu)a$, $\lambda(a + b) = \lambda a + \lambda b$ and $(\lambda + \mu)a = \lambda a + \mu a$ for all $\lambda, \mu \in F$ and $a, b \in R$. These are all trivial if either λ or μ is 0_F , reducing to things like $0 = 0$ or $a = a$. The first two are also trivial if $\lambda = \mu = 1_F$, reducing to $a = a$ and $a + b = a + b$ respectively. So the only potential problem was the third requirement, with $\lambda = \mu = 1_F$. It reduces to $(1_F + 1_F)a = a + a$. Since the left hand side is $0_F a = 0$, the condition becomes $a + a = 0$ for all $a \in R$, and we have proved that this holds.

5. If X is any set and R any ring then the set of all functions from X to R becomes a ring if addition and multiplication of functions is defined “pointwise”. That is, fg and $f + g$ are given by $(fg)(x) = (f(x))(g(x))$ and $(f + g)(x) = f(x) + g(x)$. Take R to be the two-element field $\mathbb{F}_2 = \{0, 1\}$, and for each $A \subseteq X$ define $f_A: X \rightarrow \mathbb{F}_2$ by the rule that $f_A(x)$ is 1 if $x \in A$ and 0 if $x \notin A$. Show that $f_A f_B = f_{A \cap B}$ and $f_A + f_B = f_{A \Delta B}$ for all $A, B \subseteq X$, where Δ is the “symmetric difference” operation: $A \Delta B$ consists of the elements of A that are not in B and the elements of B that are not in A .

Solution.

Let $A, B \subseteq X$ and $x \in X$. There are four cases to be considered separately: when $x \in A$ and $x \in B$, when $x \in A$ and $x \notin B$, when $x \notin A$ and $x \in B$, and when $x \notin A$ and $x \notin B$. In the first of these cases we have $x \in A \cap B$ and $x \notin A \Delta B$; so

$$f_A(x) = f_B(x) = f_{A \cap B}(x) = 1, \quad f_{A \Delta B}(x) = 0.$$

We see that $(f_A + f_B)(x) = f_A(x) + f_B(x) = 1 + 1 = 0 = f_{A \Delta B}$, and similarly $(f_A f_B)(x) = f_A(x) f_B(x) = 1 = f_{A \cap B}(x)$. Similar proofs show that the equations $(f_A + f_B)(x) = f_{A \Delta B}$ and $(f_A f_B)(x) = f_{A \cap B}(x)$ hold in the other cases too.

6. Which of the following are rings?

- (i) The set \mathbb{R}^3 , with addition defined in the usual way, and multiplication given by $(a, b, c) \times (d, e, f) = (bf - ce, cd - af, ae - bd)$.
- (ii) The set of all rational numbers expressible in the form a/b , where a and b are integers and p does not divide b . Here p denotes a fixed prime integer, and the operations are the usual ones.
- (iii) The set of integers with a new addition \oplus and a new multiplication \otimes defined in terms of the usual operations by

$$n \oplus m = n + m + 1,$$

$$n \otimes m = n + m + nm.$$

Solution.

- (i) No, the cross product multiplication is not associative. For example,

$$((1, 0, 0) \times (1, 0, 0)) \times (0, 1, 0) = (0, 0, 0),$$

whereas

$$(1, 0, 0) \times ((1, 0, 0) \times (0, 1, 0)) = (0, -1, 0).$$

- (ii) This is a ring. The fact that ordinary addition and multiplication satisfy all the ring axioms (associativity and so forth) is a familiar triviality, but what does need checking is that ordinary addition and multiplication are genuinely operations on this set. That is, you must show that sums and products of numbers in this set are in this set. So, assume that x and y are such numbers. That is, $x = a/b$ and $y = c/d$ for some integers a, b, c and d , with b and d not divisible by p . Now $xy = ac/bd$, and $x + y = (ad + bc)/bd$, and since b and d are not divisible by p it follows that bd is not divisible by p . So both xy and $x + y$ are expressible as fractions with denominator not divisible by p , as required.
- (iii) This is also a ring; in fact, it is really just the ordinary ring of integers in disguise. Let $f: \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by $f(n) = n - 1$ for all n . Then f is clearly a bijective function. Now we find that for all $n, m \in \mathbb{Z}$,

$$f(n) \oplus f(m) = (n - 1) + (m - 1) + 1 = n + m - 1 = f(n + m)$$

and similarly

$$f(n) \otimes f(m) = (n - 1)(m - 1) + (n - 1) + (m - 1) = nm - 1 = f(nm),$$

and these facts make it easy to check that \oplus and \otimes satisfy all the ring axioms. What we have shown can be expressed as follows: if we change our notation for the integers so that the number which is written as 0 in the usual notation is written instead as 1, and the number 1 (in the usual notation) is written as 2 (in the new notation), and 2 (usual notation) becomes 3 (new notation), and so on, then we will find that $4 \oplus 3 = 7$, and $5 \otimes 2 = 10$; indeed, in all cases $n \oplus m$ and $n \otimes m$ will give the same answers as do $n + m$ and nm when the usual notation is used. Since ordinary multiplication and addition satisfy the ring axioms, it follows that \otimes and \oplus do.

7. Let C be a cyclic group of order n (so that $C = \{1, x, \dots, x^{n-1}\}$ and $x^n = 1$.) The group algebra $\mathbb{R}C$ consists of all formal linear combinations $\sum_{i=0}^{n-1} \lambda_i x^i$, with $\lambda_i \in \mathbb{R}$, with addition, multiplication and scalar multiplication defined so that all the ring and vector space axioms are satisfied. Show that $\mathbb{R}C$ is not an integral domain.

Solution.

By definition, two “formal linear combinations” $\sum_{i=0}^{n-1} \lambda_i x^i$ and $\sum_{i=0}^{n-1} \mu_i x^i$ are only equal if $\lambda_i = \mu_i$ for all i . So $\sum_{i=0}^{n-1} 1x^i \neq \sum_{i=0}^{n-1} 0x^i$. This latter element is the zero of

$\mathbb{R}C$. So I am saying that, by definition, $1 + x + x^2 + \dots + x^{n-1} \neq 0$. But now

$$x(1 + x + \dots + x^{n-1}) = x + x^2 + \dots + x^n = 1 + x + \dots + x^{n-1} = 1(1 + x + \dots + x^{n-1}).$$

If $\mathbb{R}C$ were an integral domain we could cancel, and deduce that $x = 1$. Since $x \neq 1$, $\mathbb{R}C$ is not an integral domain.