

# Algebraic Structures

GCS

14-xi-11

## Groups

A *group* is a set  $G$  equipped with *binary operation*  $*$  (so if  $a, b \in G$ , then  $a * b \in G$ ), obeying three conditions:

1. If  $a, b, c \in G$ , then  $(a * b) * c = a * (b * c)$  (associative axiom)
2. There is  $e \in G$  such that  $e * x = x * e = x$  for each  $x \in G$ .
3. If  $a \in G$ , then there is  $a' \in G$  such that  $a * a' = a' * a = e$ .

## Observations

1. The set  $G$  can be finite or infinite, but it cannot be empty, because it contains  $e$ .
2. It is easy to prove cancellation laws, so if  $x, y, z \in G$  and either  $x * y = x * z$  or  $y * x = z * x$ , then  $y = z$  (see Problem Sheet 6).
3. If  $e' \in G$  and  $e' * x = x$  for some  $x \in G$ , then  $e' * x = e * x$  so  $e' = e$ . Similarly if there is  $y \in G$  such that  $y * e' = y = y * e$ , then  $e' = e$ . *So if an element behaves just a little bit like  $e$ , then it is  $e$ . In particular, we can talk about **the** two-sided identity element rather than **a** two-sided identity elements, and you do not change the original axiom system at all if you insist that there is a **unique** two-sided identity element.*
4. In commutative (i.e. abelian) groups we often write the operation as  $+$  and use  $0$  for  $e$ .
5. Among experts, the standard notation for  $a * b$  is  $ab$ , so the operation is written as the empty sign.
6. Suppose that  $a, b_1, b_2 \in G$  and  $a * b_1 = a * b_2 = e$  (or  $b_1 * a = b_2 * a = e$ ), then the cancellation law of Observation 2 applies, and  $b_1 = b_2$ . *The third group axiom guarantees the existence of a two-sided multiplicative inverse  $a'$  for each  $a \in G$ .*

This Observation ensures that this inverse for  $a$  is unique, and it makes sense to call it **the** inverse of  $a$ .

7. If  $G$  is being written additively, it is usual to write the inverse of  $a \in G$  as  $-a$ .
8. If  $G$  is being written using the operation  $*$ , or just using juxtaposition, then the inverse of  $a \in G$  is usually written  $a^{-1}$ .
9. Note that for any  $a \in G$ , we have  $a * a^{-1} = e$ , so by Observation 6, the inverse of  $a^{-1}$  is  $a$ , or if you prefer,  $(a^{-1})^{-1} = a$ .
10. The associative law ensures that brackets are irrelevant, so for example if  $a, b, c, d \in G$ , then  $(a*b)*(c*d) = (((a*b)*c)*d)$ . Therefore brackets may be unambiguously omitted, so we write either of our examples as  $a*b*c*d$ . The idle reader may care to regard this as “obvious”, but there is a proof in my *Introductory Mathematics: Algebra and Analysis* by induction.
11. If  $g \in G$ , let  $g^0 = e$  (by definition), and if  $n \in \mathbb{N}$  define  $g^n = g * g^{n-1}$  and define  $g^{-n} = g^{-1} * g^{1-n}$ . The following laws then hold:
  - (a) For all  $m, n \in \mathbb{Z}$  we have  $g^m g^n = g^{m+n}$ .
  - (b) For all  $m, n \in \mathbb{Z}$  we have  $(g^m)^n = g^{mn} = (g^n)^m$ .
  - (c) For all  $m \in \mathbb{Z}$  we have  $g^{-m} = (g^{-1})^m = (g^m)^{-1}$ .

Credulous readers can skip by, since they have always known these statements to be true. However, proper students may be punished for their inquisitiveness because proofs of these elementary facts, unless very well designed, can be fiddly.

12. If  $G$  is a group and  $g \in G$ , then there may be a non-empty set of positive integers  $k$  for which  $g^k = e$ . If so, the smallest such positive integer is written  $o(g)$ , and is called the *order of  $G$*  and we say that  $g$  has *finite order*.
13. If  $G$  is a finite group, then every element of  $G$  has finite order (see Problem Sheet 6).
14. If  $G$  is a group and  $g \in G$  is an element of finite order, then the elements  $g^0 = e, g^1 = g, g^2, \dots, g^{o(g)-1}$  are distinct and form a group in their own right. To see distinctness, suppose that  $g^i = g^j$  with  $0 \leq i < j \leq o(g) - 1$ , then postmultiplying by  $g^{-i}$ , we find  $g^{j-i} = e$  but  $0 < j-i < o(g)$ , and this violates the definition of  $o(g)$ . This subset  $\{g^i \mid 0 \leq i < o(g)\}$  of  $G$  has size  $o(g)$  (we now know that the elements are distinct so we can say this with confidence). It is closed under the operation  $*$  because  $g^{o(g)} = e$ . Associativity comes for free because  $*$  is an associative operation on  $G$ . Finally,  $g^{-1} = g^{o(g)-1}$  so  $(g^m)^{-1} = (g^{-1})^m = (g^{o(g)-1})^m$  so our set is closed under both the group operation and inversion.

15. Suppose that  $G_1, G_2, \dots, G_k$  are groups, with operations denoted  $*_1, *_2, \dots, *_k$  and identity elements  $e_1, e_2, \dots, e_k$ , then there is a natural group structure on  $G = G_1 \times G_2 \times \dots \times G_k$  defined as follows; if  $g = (g_1, g_2, \dots, g_k), h = (h_1, h_2, \dots, h_k) \in G$ , then  $g * h$  is defined to be  $(g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_k *_k h_k)$ . The identity element is  $e = (e_1, e_2, \dots, e_k)$  and  $g^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_k^{-1})$ .

## Rings

The minimalist (Spartan) definition of a ring is this. A *ring* is a set  $R$  equipped with an operation  $+$  and an identity element  $0$ , also equipped with a multiplication  $\cdot : R \times R \rightarrow R$  which distributes over addition on both sides. This means that if  $r, s, t \in R$ , then  $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$  and  $(s + t) \cdot r = (s \cdot r) + (t \cdot r)$ .

We are not content with this, and so we will insist on a more luxurious notion of a ring  $R$ . Our rings have not only the structure mentioned already but much, much more:

- (a) The multiplication  $\cdot$  must be both associative and commutative.
- (b) There must be a (two-sided) multiplicative identity  $1$ .

## Observations

1. Good prototypes for rings include  $\mathbb{Z}$ ,  $\mathbb{Z}_6$ , and polynomials in countably many commuting formal “variables”  $X_1, X_2, X_3, \dots$  with coefficients in your favourite ring, say  $\mathbb{Z}_{100}$ .
2. Consider a ring of the form  $\{0\}$  where  $0 + 0 = 0$  and  $0 \cdot 0 = 0$ . In this ring,  $1 = 0$ .
3. Suppose that  $e \in R$  and  $e \cdot x = x$  for all  $x \in R$ , then  $e = e \cdot 1 = 1$ .
4. In any ring  $R$ , if  $r \in R$ , then  $0 \cdot r = 0$ . This was proved in lectures.
5. This was not proved in lectures. If  $r \in R$ , then  $(-1) \cdot r = -r$ . Here  $-1$  is the (unique) additive inverse of  $1$ , and more generally,  $-r$  is the additive inverse of  $r$ . Here is a proof.  $0 = 1 + (-1)$  is the definition of  $-1$ . If  $r \in R$  we have  $0 \cdot r = (1 + (-1)) \cdot r = (1 \cdot r) + ((-1) \cdot r)$ . However, we proved in lectures that  $0 \cdot r = 0$ , so  $(-1) \cdot r$  is the (unique) additive inverse of  $r$ , that is  $(-1) \cdot r = -r$  as required.
6. More generally, if  $r, s \in R$ , then  $(-r) \cdot s = -(r \cdot s) = r \cdot (-s)$ . The proof is very similar to that of Observation 5.
7. Suppose that  $r, s \in R$ , then  $(-r) \cdot (-s) = -(r \cdot (-s)) = -(-(r \cdot s)) = r \cdot s$ . Please supply the justifications for each step.

## Special Rings

### Integral Domains

An *integral domain*  $R$  is a ring (so the multiplication is commutative, associative and with 1) in which both (a)  $0 \neq 1$  and (b) if  $r, s \in R$  and  $rs = 0$ , then either  $r = 0$  or  $s = 0$  (or both).

We proved in lectures that in an integral domain, cancellation by non-zero elements is possible. Thus if  $r, s, t \in R$  with  $r \neq 0$ , and  $rs = rt$  (or  $sr = tr$ ), then  $t = r$ .

Examples of rings include  $\mathbb{Z}$  and  $\mathbb{R}$ . The ring  $\mathbb{Z}_n$  is not an integral domain unless  $n$  is prime, in which case it is.

### Fields

A *field*  $F$  is a ring (so the multiplication is commutative, associative and with 1) in which both (a)  $0 \neq 1$  and (b) if  $r \in R \setminus \{0\}$ , then there is  $s \in R$  such that  $rs = 1$ .

Thus in a field, non-zero elements are divisors of 1.

### Observations

1. All fields are integral domains, but not all integral domains are fields (the ring of integers  $\mathbb{Z}$  is an example).
2. A finite integral domain  $R$  must be a field. This result has a neat proof. Suppose that  $r \in R$  and  $r \neq 0$ . It suffices to show that  $r$  must be a divisor of 1 (i.e. that it must have a multiplicative inverse). Define a map  $\theta_r : R \rightarrow R$  by  $x \mapsto rx \forall x \in R$ . Now if  $rx_1 = rx_2$ , then  $r(x_1 - x_2) = 0$  but  $r \neq 0$  and  $R$  is an integral domain, so  $x_1 = x_2$  and so  $\theta_r$  is injective. The set  $R$  is finite, so  $\theta_r$  is bijective and  $1 \in \text{Im } \theta_r$ , so there is  $s \in R$  such that  $\theta_r(s) = 1$  i.e.  $rs = 1$ .
3. A ring which is a direct sum of two non-zero rings cannot be an integral domain. Suppose that  $R = S \oplus T$ . Notice that  $(0, 1) \cdot (1, 0) = (0, 0) = 0_R$ . However,  $S$  is not the zero ring so there is  $s \in S$  with  $s \neq 0$ . Therefore  $1 \neq 0$  for otherwise  $s = 1 \cdot s = 0 \cdot s = 0$  (the final equality is by Observation 4 of the section headed Rings). Therefore  $(1, 0) \neq 0_R$ . Similarly  $(0, 1) \neq 0_R$ , but  $(1, 0) \cdot (0, 1) = (0, 0) = 0_R$ .