

Contents

1	Introduction to Groups	1
1.1	Basic Axioms and Examples	1

1 Introduction to Groups

1.1 Basic Axioms and Examples

3 & 4	1
5	1
7	1
15	2
16	2
17	2
19	2
20	2

3 & 4

Notice that for any integers x, y the following properties holds for their residue classes mod n :

$$\overline{x * y} = \bar{x} * \bar{y} \quad \overline{x + y} = \bar{x} + \bar{y}$$

The associativity of multiplication and addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ follows from these facts and the associativity of multiplication and addition over the integers. Let $a, b, c \in \mathbb{Z}$.

$$\begin{aligned} (\bar{x} + \bar{y}) + \bar{z} &= \overline{(\bar{x} + \bar{y}) + \bar{z}} \\ &= \overline{\bar{x} + (\bar{y} + \bar{z})} \\ &= \bar{x} + (\bar{y} + \bar{z}) \end{aligned}$$

The argument is essentially the same for multiplication.

5

Let $n > 1$. Now consider $\bar{0} \in \mathbb{Z}/n\mathbb{Z}$. It's not possible for $\bar{0}$ to have a multiplicative inverse, because any value multiplied by $\bar{0}$ is $\bar{0}$. Thus $\mathbb{Z}/n\mathbb{Z}$ for n greater than one are not groups.

7

Define for any real number x :

$$\bar{x} = x - [x]$$

Notice that for any $x, y \in G$

$$x * y = x + y - [x + y] = \overline{x + y}$$

The associativity and commutativity of $*$ follow from this definition (combined with the associativity and commutativity of addition).

$$x * y = \bar{x} * \bar{y} = \overline{\bar{x} + \bar{y}}$$

- well defined.

If $x = x'$ and $y = y'$, then

$$x * y = x + y - [x + y] = x' + y' - [x' + y'] = x' * y'$$

- binary operation/closure

$x * y$ is at least 0 (when $x+y$ is an integer) and no more than one. Thus $x * y \in G$

- associative

$$(x \star y) \star z = \overline{(x+y)} + z = \overline{x+(y+z)} = x \star (y \star z)$$

- commutative

$$x \star y = \overline{x+y} = \overline{y+x} = y \star x$$

- identity

For any x in G :

$$x \star 0 = \overline{x+0} = x$$

- every element has an inverse

Let x be an arbitrary element of G . Then $1-x$ is its inverse:

$$x \star (1-x) = \overline{x+1-x} = \overline{1} = 0$$

9

- (a) ...
- (b)

– associativity, binary operation ...

– identity element

For any x in G , $x \star 1 = x$ so 1 is identity

– everything has inverse

Let $a + b\sqrt{2} \in G$. We want to show some $x, y \in \mathbb{Q}$ exist such that

$$(a + b\sqrt{2})(x + y\sqrt{2}) = ax + b\sqrt{2}y\sqrt{2} + ay\sqrt{2} + b\sqrt{2}ax = ax + 2by + (ay + bax)\sqrt{2} = 1$$

For this to be the case, the following system of equations must be satisfiable:

$$ax + 2by = 1 \quad ay + bax = 0$$

... (this actually seems pretty hard because for some values of a, b it seems like there is no solution?)

15

We can show

Notice:

$$\begin{aligned} (a_1 a_2 \cdots a_n) \cdot (a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}) &= (a_1 a_2 \cdots a_{n-1}) a_n \cdot a_n^{-1} (a_{n-1}^{-1} \cdots a_1^{-1}) \\ &= (a_1 a_2 \cdots a_{n-1}) \cdot (a_{n-1}^{-1} \cdots a_1^{-1}) \end{aligned}$$

16

First direction: If the order of an element of a group is 2 then by definition, that element squared is 1. If the order is 1, then that element to any power including 2 is 1.

Second direction: Suppose x doesn't have order 1 or 2 (in other words x has order greater than 2). Thus the smallest positive integer n such that $x^n = 1$ is greater than 2. It can't be the case then that $x^2 = 1$.

17

19

20