Contents

1 Introduction to Groups

1.1 Basic Axioms and Examples

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

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

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 $a, b, c \in \mathbb{Z}$.

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

The argument is essentially the same for multiplication.

1.1.5

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.

1.1.7

Define for any real number x:

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

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

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

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

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

- well defined.

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

  $$x \star y = x + y - [x + y] = x' + y' - [x' + y'] = x' \star y'$$

- binary operation/closure

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

- 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:

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

9

- (a) ...
- (b)
  - associativity, binary operation ...
  - identity element

    For any x in G, x*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:

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

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

1.1.15

We can show

Notice:

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

1.1.16

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 $x^2 = 1$.

1.1.17

1.1.19

1.1.20

1.2 Matrix Groups

1.2.1

Prove that $|GL_2(\mathbb{F})| = 6$

1.2.2

Write out all the elements of $GL_2(F_2)$ and compute the order of each element.

1.2.3

Show that $GL_2(\mathbb{F})$ is non-abelian.

1.2.4

Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

1.2.5

Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements

1.2.6

If $|F| = q$ is finite prove that $GL_n(F) < q^{n^2}$.

1.2.7

Let p be a prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$. (do not just quote the order formula in this section). [Subtract the number of 2 x 2 matrices over $\mathbb{F}_p$. You may use tha fact that a 2 x 2 matricx is not invertible if and only if one row is a muliple of the other.]

1.2.8

Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.

1.2.9

Prove that the binary operation of matrix muliplication of 2 x 2 matricies iwth real entities is associative

1.2.10

Let $H(F) = \{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} | a, b, c, d \in F \}$ – called the Heisenberg group over F. Let $X = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ and $Y = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix}$ be elements of $H(F)$.

1. Compute the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit maricies such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).
2. Find and explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverse.
3. Prove the associative law for $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$.
4. Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.
5. Prove that every nonidentity elements of the group $H(\mathbb{R})$ has infinite order.