Contents

1 Introduction to Groups

1.1 Basic Axioms and Examples

1.1.3

Recall multiplication and addition are defined as follows over residue classes:

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

The associativity of muliplication and addition follows directly from these definitions and the associativity of these operations on the integers. Let $a, b, c \in \mathbb{Z}$.

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

1.1.4

The argument is essentially the same for multiplication.

1.1.5

All residue classes mod n where $n > 1$ do not form a group under multiplication because $\bar{0}$ is an element of all of them and it can not have an inverse. If an inverse, $\bar{a}$, were to exist, $\bar{0} * \bar{a} = \bar{1}$. However, $\bar{0} * \bar{a} = \overline{0 * a} = \bar{0}$.

1.1.7

We can simplify this problem by defining a new operation over real numbers:

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

$\star$ can equivalently be defined in terms of this operation:

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

- 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

  Subtracting the integer part from a real number always results in a value less than 1 and no less than 0, i.e. $0 \leq \bar{x} = x - [x] < 1$. It follows that $0 \leq \overline{x+y} = x \star y < 1$ and thus $\star$ is closed under G

- associative

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

- commutative

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

- identity

  0 is the identity element. For any x in G:

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

- every element has an inverse

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

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

9

Let $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

- (a) prove G is a group under addition.

  ... (skipping because it doesn't seem to interesting)

- (b) prove that the nonzero elements of G are a group under multiplication

  - associativity, binary operation

    ... (skipping these as well because they seem boring)

  - identity element

    $1 + 0 * \sqrt{2} = 1$ is the identity element. Let $a + b\sqrt{2} \in G$. Then

$$1 * (a + b\sqrt{2}) = (a + b\sqrt{2}) * 1 = a + b\sqrt{2}$$

  - everything has inverse

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

$$\begin{aligned}(a + b\sqrt{2})(x + y\sqrt{2}) &= 1 \\ ax + ay\sqrt{2} + b\sqrt{2}x + b\sqrt{2}y\sqrt{2} &= 1 \\ ax + ay\sqrt{2} + b\sqrt{2}x + 2by &= 1 \\ ax + 2by + (ay + bx)\sqrt{2} &= 1\end{aligned}$$

    Equivalently:

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

    Solving this system of equations with a wolframalpha (https://www.wolframalpha.com/input?i=ax+%2B+2by+%3D+1+%5Cquad+%5Cquad%2C++ay+%2B+bx+%3D+0) gives:

$$a = 0, \quad x = 0, \quad b \neq 0, \quad y = \frac{1}{2b}$$

$$a^2 - 2b^2 \neq 0, \quad x = \frac{a}{a^2 - 2b^2}, \quad a \neq 0, \quad y = \frac{b}{2b^2 - a^2}$$

asking chatgpt to turn that into a cases format gave the following which I don't think is really correct:

$$\begin{cases} x = 0,\ y = \dfrac{1}{2b}, & a = 0,\ b \neq 0, \\ x = \dfrac{a}{a^2 - 2b^2},\ y = \dfrac{b}{2b^2 - a^2}, & a \neq 0,\ a^2 - 2b^2 \neq 0. \end{cases}$$

after spending a long time leading/dragging chatgpt in the right dircetion I was able to get it to output what I think is the most concise clean and correct solution:

$$(x, y) = \frac{1}{a^2 - 2b^2}\,(a,\ -b) \qquad \text{for } a, b \in \mathbb{Q},\ (a, b) \neq (0, 0).$$

I won't exactly prove why that's the case but I will note that the that $a^2 - 2b^2 \neq 0$ case is redundant. That's because $a = \sqrt{2}b$ is not possible for rational a and b. Furthermore $(a, b) = (0, 0)$ is not relevant since we were only intrested in the nonzero elements of G. Thus we can always find a multiplicative inverse for any of the nonzero elements of G with the following formula:

$$(x, y) = \frac{1}{a^2 - 2b^2}\,(a,\ -b)$$

Aside

This is an interesting system of equations for CAS. It's really not that complicated, yet neither wolframalpha or sympy handeled it super easily. It would be nice to be able to assume the variables involved were rational and just immediately get out the most concise solution and be sure it was correct.

1.1.15

I though about this for a while and I like August's solution so maybe I'll do something along the same lines. I was actually having a bit of trouble coming up with something that wasn't needless verbose. That being said sometimes doing something concise but non standard is actually harder to read.

- n=1
$$(a_1)^{-1}a_1^{-1} = 1 = a_1^{-1}(a_1)^{-1}$$
- Assume $(a_1 \cdots a_{n-1})^{-1} = a_{n-1}^{-1} \cdots a_1^{-1}$. We want to show $(a_1 \cdots a_n)^{-1} = (a_n^{-1} \cdots a_n^{-1})$.

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

Similarly:

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

1.1.16

Let x be an element of G. Prove that $x^2 = 1 \iff |x| = 1 \wedge |x| = 2$

- $x^2 = 1 \implies |x| = 1 \wedge |x| = 2$

  Suppose toc x doesn't have order 1 or 2 (in other words x has order greater than 2). By defenition, the smallest positive integer n such that $x^n = 1$ is greater than 2. It can't be the case then that $x^2 = 1$ and so we have reached a contradiction.

- $|x| = 1 \wedge |x| = 2 \implies x^2 = 1$

  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.

1.1.17

Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Suppose $|x| = n$. By definition of order this means $x^n = 1$. Thus:

$$xx^{n-1} = x^{n-1}x = x^n = 1$$

In other words, x^{n-1} is the inverse of x.

1.1.19

Let x be an element of a group and a and b be positive integers. Prove:

- (a) $x^a x^b = x^{a+b}$ and $(x^a)^b = x^{ab}$

  We prove $x^a x^b = x^{a+b}$ by doing induction on b:

  - b= 1

    $$x^a x^1 = a^{a+1}$$

  - Assume $x^a x^n = x^{a+n}$. We want to show $x^a x^{n+1} = x^{a+n+1}$

    $$\begin{aligned} x^a x^n &= x^{a+n} \\ x^a x^n x &= x^{a+n} x \\ x^a x^{n+1} &= x^{a+n+1} \end{aligned}$$

  We prove $(x^a)^b = x^{ab}$ by induction on b:

  - n=1

    $$(x^a)^1 = a^a = x^{a*1}$$

  - Assume $(x^a)^n = x^{an}$. We want to show $(x^a)^{n+1} = x^{a(n+1)}$.

    $$\begin{aligned} (x^a)^n &= x^{an} \\ (x^a)^n (x^a) &= x^{an}(x^a) \\ (x^a)^n (x^a)^1 &= x^{an}(x^a)^1 \\ (x^a)^{n+1} &= x^{an+a} \quad \text{by what we just proved earlier} \\ (x^a)^{n+1} &= x^{a(n+1)} \end{aligned}$$

- (b)$(x^a)^{-1} = x^{-a}$

  We prove this by induction on a:

  - a=1

    $$(x^1)^{-1} = x^{-1}$$

  - Assume $(x^n)^{-1} = x^{-n}$. We want to show $(x^{n+1})^{-1} = x^{-n-1}$.

    $$\begin{aligned} x^n x^{-n} &= 1 \\ x x^n x^{-n} &= x \\ x^{n+1} x^{-n} x^{-1} &= x x^{-1} \\ x^{n+1} x^{-n-1} &= 1 \end{aligned}$$

- (c) show a is true for integers a and b that don't have to be positive

  ok been thinking about this. if a and b are both negative it's pretty straightforward since there's symetry in the definitions of x^{-n} and x^n.

  the other case is when one is positive and the other is negative. the maginitude of the exponents are equal or one is bigger than the other. We don't have to do a case split on which one is bigger. we can use the symetry I talked about earier so we can assume either the positive or negative is grearer or equal to the other (in magnatude). we can split the bigger one up into a part that's equal to the smaller one and the remainer. then we apply problem 15.

  - Case 1: $a, b \geq 0$

    It suffices to show the statement holds if $a = 0 \vee b = 0$ since we proved the case where they're both positive in part (a). If a=0:

    $$x^a x^b = x^b = x^{a+b} \quad \text{and} \quad (x^a)^b = 1^b = 1 = 1^0 = x^{ab}$$

    Similarly, if b=0:

    $$x^a x^b = x^a = x^{a+b} \quad \text{and} \quad (x^a)^b = (x^a)^0 = 1 = 1^0 = x^{ab}$$

  - Case 2: both are negative

    We can rewrite the equations so that they have positive exponents with part (b) so that part (a) applies. With the first equation we substitute $x = (x^{-1})^{-1}$ into the first equation from part (a):

    $$\begin{aligned} ((x^{-1})^{-1})^a((x^{-1})^{-1})^b &= ((x^{-1})^{-1})^{a+b} \\ (x^{-1})^{-a}(x^{-1})^{-b} &= (x^{-1})^{-a-b} \\ (x^{-1})^{a'}(x^{-1})^{b'} &= (x^{-1})^{a'+b'} \end{aligned}$$

    Similarly:

    $$\begin{aligned} (x^a)^b &= x^{ab} \\ (((x^{-a})^{-1})^{-1})^{-b} &= x^{ab} \\ (x^{-a})^{-b} &= x^{(-a)(-b)} \\ (x^{a'})^{b'} &= x^{a'b'} \end{aligned}$$

  - Case 3: one is non-negative and the other is non-positive.

    First, notice that swapping a and b doesn't change anything:

    $$x^a x^b = x^{a+b} = x^{b+a} = x^b x^a$$

    Similarly:

    $$(x^a)^b = x^{ab} = x^{ba} = (x^b)^a$$

    It's either the case that $|a| \geq |b|$ or $|a| \leq |b|$. Suppose wlog the former is true. Now, recall that in case 2 we were able to flip the signs of all the exponents. This means that if we want a to be non-negative and b to be negative but the opposite is true, we can flip the signs to get what we want. Assume wlog that $a \geq 0 \geq b$.
    Since $|a| \geq |b|$ and $a \geq 0 \geq b$ we know

    $$a = -b + r$$

    where r and -b are non-negative integers.

    $$\begin{aligned} x^a x^b &= x^{a+b} \\ x^{-b+r} x^b &= x^{-b+r+b} \\ x^{-b+r} x^b &= x^r \\ x^r x^{-b} x^b &= x^r \qquad \text{by part (a)} \\ x^r &= x^r \qquad \text{by problem 15} \end{aligned}$$

With the other equation we can rearrange things so that only positive exponents are involved:

$$(x^a)^b = x^{ab}$$
$$((x^{-1})^a)^{-b} = (x^{-1})^{a(-b)}$$
$$((x')^a)^{b'} = (x')^{ab'}$$

In this rearranged form it's clear that it's true by a simple application of part (a)

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.