

My abstract algebra exercises

Evgeny Markin

2023

Contents

0.1	Basics	2
0.1.1	2
0.1.2	2
0.1.3	3
0.1.4	3
0.1.5	3
0.1.6	4
0.1.7	4
0.2	Properties of the Integers	4
0.2.1	4
0.2.2	5
0.2.3	5
0.2.4	5
0.2.5	6
0.2.6	6
0.2.7	6
0.2.8	7
0.3	$\mathbb{Z}/n\mathbb{Z}$: The Integers Modulo n	7
0.3.1	7
0.3.2	7
0.3.3	7
0.3.4	8
0.3.5	8
0.3.6	8
0.3.7	9
0.3.8	9
0.3.9	9
1	Introduction to Groups	10
1.1	Basic Axioms and Examples	10
1.2	Dihedral Groups	18

Preliminaries

0.1 Basics

0.1.1

Determine which of the following elements of A lie in B

M is defined to be

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$B = \{x \in A : MX = XM\}$$

thus all of the following are in B .

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

0.1.2

Prove that $P, Q \in B \Rightarrow P + Q \in B$

Suppose that $P, Q \in B$. Then we follow that

$$(P + Q)M = PM + QM = QM + PM = (Q + P)M$$

where we've used distributive and commutativity under addition for matrices

0.1.3

Prove that $P, Q \in B \Rightarrow PQ \in B$

Suppose that $P, Q \in B$. Thus we follow that $PM = MP$ and $QM = MQ$. Thus

$$(PQ)M = PQM = P(QM) = P(MQ) = PMQ = (PM)Q = (MP)Q = M(PQ)$$

as desired.

0.1.4

Find conditions on p, q, r, s , which determine precisely when

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in B$$

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix}$$

thus we follow that we need to have

$$\begin{pmatrix} p+r & q+s \\ r & s \end{pmatrix} = \begin{pmatrix} p & p+q \\ r & r+s \end{pmatrix}$$

thus we follow that the matrix is in B if and only if $r = 0$ and $p = s$. (ocave seems to support this point).

0.1.5

Determine whether the following functions f are well-defined:

(a)

$$f : Q \rightarrow Z : f(a/b) = a$$

If we assume that a/b is in form, where $b > 0$ and a/b in their lower terms, then the function is well-defined. Otherwise, we've got that

$$2/4 = 1/2$$

but

$$f(2/4) = 2 \neq 1 = f(1/2)$$

(b)

$$f : Q \rightarrow Q : f(a/b) = a^2/b^2$$

is indeed well-defined, since for every $a \in Q$ there is only one square.

0.1.6

Determine whether the function $f : \mathbb{R}^+ \rightarrow \mathbb{Z}$ defined by mapping a real number r to the first digit to the right of the decimal point in a decimal expansion of r is well-defined.

This is a somewhat trick question, since we've got that

$$1 = 0.99999999\ldots$$

which in this case gives us that f is not well-defined.

0.1.7

Let $f : A \rightarrow B$ be a surjective map of sets. Prove that the relation

$$a \sim b \Leftrightarrow f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of f .

$$f(a) = f(a) \Rightarrow a \sim a$$

$$(f(a) = f(b) \wedge f(b) = f(c) \Rightarrow f(a) = f(c)) \Rightarrow (a \sim b \wedge b \sim c \Rightarrow a \sim c)$$

$$a \sim b \Rightarrow f(a) = f(b) \Rightarrow f(b) = f(a) \Rightarrow b \sim a$$

which gives us reflexive, transitive and symmetric properties, thus \sim is an equivalence relation.

We follow that if $x \in B$ and $a, b \in f^{-1}(\{x\})$, then $a \sim b$ by definition. Suppose that $a \sim b$. Then we follow that $f(a) = f(b)$, therefore $a \in f^{-1}(\{f(a)\}) \wedge b \in f^{-1}(\{f(a)\})$. Thus we follow that if $a \sim b$, then they are fibers for the same value. Thus we follow that $a \sim b$ if and only if $(\exists x \in B)(a, b \in f^{-1}(\{x\}))$. Thus we follow that fibers of f are indeed the equivalence classes for \sim .

0.2 Properties of the Integers**0.2.1**

Find GCD and LCM for following numbers and find integers x and y such that $ax + by = \gcd(a, b)$

```
gcd:   1; lcm:       260, 2 * 20 + -3 * 13 = 1
gcd:   3; lcm:      8556, 27 * 69 + -5 * 372 = 3
gcd:  11; lcm:     19800, 8 * 792 + -23 * 275 = 11
gcd:   3; lcm:  21540381, -126 * 11391 + 253 * 5673 = 3
gcd:   1; lcm:   2759487, -105 * 1761 + 118 * 1567 = 1
gcd: 691; lcm:  44693880, -17 * 507885 + 142 * 60808 = 691
```

0.2.2

Prove that if the integer k divides the integers a and b , then k divides $as + bt$ for every pair of integers s and t

We follow that because k divides both a and b it also divides (a, b) . Since (a, b) divides both a and b we follow that there exist $q, w \in \mathbb{Z}$ such that $a = q(a, b)$, $b = w(a, b)$. Thus

$$as + bt = q(a, b) + w(a, b) = (q + w)(a, b)$$

thus we follow that (a, b) divides $as + bt$. Since $|$ is transitive, we follow that $k|(a, b)$ and $(a, b)|as + bt$ implies that $k|as + bt$, as desired.

(We could've actually skip this part, don't know why I've used it)

0.2.3

Let a, b, N be fixed integers with $a, b \neq 0$ and let $d = (a, b)$. Suppose that $x_0, y_0 \in \mathbb{Z}$ are such that $ax_0 + by_0 = N$. Prove that

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = N$$

$$\begin{aligned} a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) &= ax_0 + a\frac{b}{d}t + by_0 - b\frac{a}{d}t = ax_0 + by_0 + t(\frac{ab}{d} - \frac{ab}{d}) = \\ &= ax_0 + by_0 + t(0) = N + 0 = N \end{aligned}$$

0.2.4

Determine the value $\phi(n)$ for each integer $n \leq 30$ where ϕ denotes the Euler ϕ -function

$\phi(1) = 1$
 $\phi(2) = 1$
 $\phi(3) = 2$
 $\phi(4) = 2$
 $\phi(5) = 4$
 $\phi(6) = 2$
 $\phi(7) = 6$
 $\phi(8) = 4$
 $\phi(9) = 6$
 $\phi(10) = 4$
 $\phi(11) = 10$
 $\phi(12) = 4$
 $\phi(13) = 12$

$\text{phi}(14) = 6$
 $\text{phi}(15) = 8$
 $\text{phi}(16) = 8$
 $\text{phi}(17) = 16$
 $\text{phi}(18) = 6$
 $\text{phi}(19) = 18$
 $\text{phi}(20) = 8$
 $\text{phi}(21) = 12$
 $\text{phi}(22) = 10$
 $\text{phi}(23) = 22$
 $\text{phi}(24) = 8$
 $\text{phi}(25) = 20$
 $\text{phi}(26) = 12$
 $\text{phi}(27) = 18$
 $\text{phi}(28) = 12$
 $\text{phi}(29) = 28$
 $\text{phi}(30) = 8$

0.2.5

Prove the WOP of Z by induction and prove the minimal element is and prove the minimal element is unique.

GOTO set theory book

0.2.6

If f is a prime prove that there do not exist nonzero integers a and b such that $a^2 = pb^2$

We follow that a and b can be represented as multiples of primes. Therefore the powers of primes, that represent a^2 and b^2 are even. Since the power of p in pb^2 is not even, we follow that such numbers do not exist, as desired

0.2.7

Let p be a prime, $n \in Z^+$. Find a formula for the largest power of p which divides $n!$

We follow that every p 'th number is a multiple of p . Thus the amount of multiples of p in the list $1, 2, \dots, n$ is $\lfloor n/p \rfloor$. To those we need to add the number of multiples of p^2 , of which there will be $\lfloor n/p^2 \rfloor$, and thus we follow that the number of multiples of p in n is

$$\sum_{i=1}^n \lfloor n/p^i \rfloor$$

Since for every prime number we've got that $p^n > n$, we can follow that this formula will do.

0.2.8

Write a computer program to determine

Way ahead of you, check `congr.py` in `progs`.

0.3 Z/nZ : The Integers Modulo n **0.3.1**

Write down explicitly all the elements in the residue classes $Z/18Z$.

$$\overline{1}, \overline{2}, \dots, \overline{17}$$

0.3.2

Prove that the distinct equivalence classes in Z/nZ are precisely $\overline{0}, \dots, \overline{n-1}$.

Suppose that $q \in N$. We follow that $q = an + r$, where $0 \leq r < n$, thus we follow that $q \in \overline{r}$. Therefore every integer is in one of those sets. Since r is unique, we follow that q is only in one of those sets.

0.3.3

Prove that of $a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$ is any positive integer then $a \equiv \sum a_n \pmod{9}$.

We follow that $10 \equiv 1 \pmod{9}$, and therefore $10^n \equiv 1 \pmod{9}$ for any $n \in Z$. Thus we can follow that

$$10a_n \equiv a_n \pmod{9}$$

and in general

$$10^n a_n \equiv a_n \pmod{9}$$

therefore

$$\overline{a_n 10^n} = \overline{a_n}$$

and since

$$\sum \overline{a_n} = \overline{\sum a_n}$$

we follow the desired result.

0.3.4

Compute the remainder when 37^{100} is divided by 29

We follow that

$$37^{100} \equiv 8^{100} \pmod{29}$$

thus

$$8^1 \equiv 8 \pmod{29}$$

$$8^2 \equiv 6 \pmod{29}$$

$$8^4 \equiv 36 \equiv 7 \pmod{29}$$

$$8^8 \equiv 49 \equiv 20 \pmod{29}$$

$$8^{10} \equiv 120 \equiv 4 \pmod{29}$$

$$8^{20} \equiv 16 \pmod{29}$$

$$8^{40} \equiv 256 \equiv 24 \pmod{29}$$

$$8^{50} \equiv 96 \equiv 9 \pmod{29}$$

$$8^{100} \equiv 81 \equiv 23 \pmod{29}$$

thus we follow that 37^{100} divided by 29 gives us the answer 23.

0.3.5

$$9^{1500} = \dots 01$$

0.3.6

Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just 0 and 1

We follow that

$$0^2 = 0$$

$$1^2 = 1$$

$$2^2 = 4 \equiv 0 \pmod{4}$$

$$3^2 = 9 \equiv 1 \pmod{4}$$

so yeah

0.3.7

Prove for any integers a and b that $a^2 = b^2$ never leaves a remainder of 3 when divided by 4

From previous exercise we follow that

$$a^2 \equiv [0, 1] \pmod{4}$$

$$b^2 \equiv [0, 1] \pmod{4}$$

thus

$$a^2 + b^2 \equiv [0, 1, 2] \pmod{4}$$

0.3.8

Prove that the equation $a^2 + b^2 = 3c^2$ has no nonzero integer solutions

We follow from previous exercise that $a^2 + b^2 \equiv [0, 1, 2] \pmod{4}$, and $c^2 \equiv [0, 1] \pmod{4}$, therefore $3c^2 \equiv [0, 3] \pmod{4}$. Thus we follow that the only possible case is when $a^2 + b^2 \equiv 3c^2 \equiv 0 \pmod{4}$. Thus we follow all of the a^2 , b^2 and c^2 have the factor of 4. Thus there exist a_0, b_0, c_0 such that $a^2 = 4^n a_0^2$, $b^2 = 4^n b_0^2$, $c^2 = 4^n c_0^2$ and a_0^2, b_0^2, c_0^2 are not divisible by 4 (otherwise we get a contradiction). Thus we follow that

$$a_0^2 + b_0^2 = 3c_0^2$$

all of which are not divisible by 4, which gets us a contradiction, as desired.

0.3.9

Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8

We follow that remainders of squares of congruent classes of 8 are

$$01410141$$

thus we follow the desired conclusion.

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

Let G be a group

1.1.1

Determine which of the following binary operations are associative

(a)

$$Z$$

$$a \star b = a - b$$

$$(a - b) - c = a - b - c = a - (b + c)$$

therefore it is not associative

(b)

$$R$$

$$a \star b = a + b + ab$$

$$(a \star b) \star c = (a + b + ab) \star c = (a + b + ab) + (c) + (ca + cb + abc)$$

$$a \star (b \star c) = a \star (b + c + bc) = (a) + (b + c + bc) + (ab + ac + abc)$$

$$(a + b + ab) + (c) + (ca + cb + abc) - ((a) + (b + c + bc) + (ab + ac + abc)) = \\ = 0$$

therefore it is associative.

(c)

$$Q$$

$$a \star b = \frac{a + b}{5}$$

$$(a \star b) \star c = \frac{a+b}{5} \star c = \frac{\frac{a+b}{5} + c}{5} = \frac{a+b+5c}{25}$$

$$a \star (b \star c) = a \star \frac{b+c}{5} = \frac{a + \frac{b+c}{5}}{5} = \frac{5a+b+c}{25}$$

therefore it is not associative.

(d)

$$Z \times Z$$

$$(a, b) \star (c, d) = (ad + bc, bd)$$

$$((a, b) \star (c, d)) \star (e, f) = (ad + bc, bd) \star (e, f) = ((ad + bc)f + bde, bdf) = (adf + bcf + bde, bdf)$$

$$(a, b) \star ((c, d) \star (e, f)) = (a, b) \star (cf + de, df) = (adf + b(cf + de), bdf) = (adf + bcf + bde, bdf)$$

therefore it is associative.

(e)

$$Q \setminus \{0\}$$

$$a \star b = \frac{a}{b}$$

$$a \star (b \star c) = a \star \frac{b}{c} = \frac{a}{\frac{b}{c}} = \frac{ac}{b}$$

$$(a \star b) \star c = \frac{a}{b} \star c = \frac{\frac{a}{b}}{c} = \frac{ac}{b}$$

therefore it is associative.

1.1.2

Decide which of the binary operations in the preceeding exercise are commutative

b and c

1.1.3

Prove that addition of residue classes in Z/nZ is associative

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c} = \overline{a+b+c} = \overline{a+b} + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}$$

1.1.4

Prove that multiplication of residue classes in Z/nZ is associative

analogous to previous

1.1.5

Prove that for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication

We follow that there is no inverse of $\bar{0}$, $\mathbb{Z}/n\mathbb{Z}$ is not a group

1.1.6

Determine which of the following sets are groups under addition

Sums are associative for every following group, therefore I'll skip discussion about them.

(a) *Rationals, whose denominators are odd*

Is a group, denominator of the sum is a divisor of product of two odd numbers, and therefore it is odd itself, and inverses of given elements have same denominators as the elements themselves.

(b) *Rationals. whose denominators are even*

$$1/2 + 1/2 = 1/1$$

therefore it is not closed under addition, and therefore it is not a group.

(c) *The set of rational numbers of absolute value < 1*

$$0.7 + 0.7 = 1.4$$

therefore it is not closed under addition, and therefore it is not a group.

(d) *the set of rationals of absolute value ≥ 1 , together with 0*

$$-1.5 + 1 = 0.5$$

therefore it is not closed under addition, and therefore it is not a group.

(e) *the set of rationals, with denominators equal to 1 or 2 (or 3)*

Is a group under addition.

1.1.7

Let $G = \{x \in \mathbb{R} : 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$. Prove that \star is a well-defined binary operation on G and that G is an abelian group under \star .

Since $\lfloor \cdot \rfloor$ is a well-defined function, we follow that there exists unique $\lfloor x + y \rfloor$ for given $x, y \in \mathbb{R}$, and therefore $x + y - \lfloor x + y \rfloor$ is a well-defined on $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$.

Let $x, y \in G$. Then we follow that $0 \leq x + y < 2$, therefore we've got two cases: if $x + y < 1$ or $1 \leq x + y < 2$. In former case we follow that $\lfloor x + y \rfloor = 0$, therefore

$$0 \leq x \star y = x + y < 1$$

. In the latter case we've got that

$$\lfloor x + y \rfloor = 1$$

, therefore $x \star y = x + y - 1$ and thus $0 \leq x \star y = x + y - 1 < 1$. Therefore $x, y \in G \Rightarrow x \star y \in G$, therefore we can state that $\star : G \times G \rightarrow G$ is a well-defined function on G .

Thus

$$x \star (y \star z) = x \star (y + z - \lfloor y + z \rfloor) = x + y + z - \lfloor y + z \rfloor - \lfloor x + y + z - \lfloor y + z \rfloor \rfloor$$

$$(x \star y) \star z = (x + y - \lfloor x + y \rfloor) \star z = x + y + z - \lfloor x + y \rfloor - \lfloor x + y + z - \lfloor x + y \rfloor \rfloor$$

We follow that for every $n \in Z$ we've got that $\lfloor n \rfloor = n$. It is also pretty straightforward (although I can't seem to produce a concrete proof for now) to check that $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ for every $n \in Z$. Since $\lfloor x \rfloor \in Z$ for every $x \in R$ we follow that

$$\begin{aligned} (x \star y) \star z &= \\ &= x + y + z - \lfloor y + z \rfloor - \lfloor x + y + z - \lfloor y + z \rfloor \rfloor = x + y + z - \lfloor y + z \rfloor - \lfloor x + y + z \rfloor + \lfloor y + z \rfloor = \\ &= x + y + z - \lfloor x + y + z \rfloor = x + y + z - \lfloor x + y \rfloor - \lfloor x + y + z \rfloor + \lfloor x + y \rfloor = \\ &= x + y + z - \lfloor y + z \rfloor - \lfloor x + y + z - \lfloor y + z \rfloor \rfloor = x \star (y \star z) \end{aligned}$$

therefore \star is an associative function.

By definition, $0 \in G$, therefore

$$0 \star x = 0 + x + \lfloor 0 + x \rfloor = x + \lfloor x \rfloor = x = x \star 0$$

thus we've got the identity in G .

For 0 we've got that it is an inverse of itself. For every $x \in G \setminus \{0\}$ we can follow that $1 - x \in G$ therefore $1 - x \star x = x + 1 - x + \lfloor 1 \rfloor = 0$ therefore for every $x \in G$ we've got the identity.

Thus we can follow that $\langle G, \star \rangle$ is indeed a group.

We also follow that $x \star y = x + y - \lfloor x + y \rfloor = y + x - \lfloor y + x \rfloor = y \star x$ therefore given group is also abelian, as desired.

1.1.9

Let $G = \{a + b\sqrt{2} \in R : a, b \in Q\}$.

Prove that G is a group under addition.

Let $x, y, z \in G$. Thus

$$x + y = a_x + b_x\sqrt{2} + a_y + b_y\sqrt{2} = (a_x + a_y) + \sqrt{2}(b_x + b_y)$$

therefore G is closed under addition, thus we follow that $+$: $G \times G \rightarrow G$. Sums are associative in general, therefore gonna skip that. 0 is the usual identity, which can be represented as $0 + 0\sqrt{2}$, thus $0 \in G$. For $x \in G$ we can define $x^{-1} = -a_x - b_x\sqrt{2}$, which is also in G . Thus we follow that $\langle G, + \rangle$ is indeed a group, as desired.

1.1.11

Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

we've got that

ord (0) = 1
ord (1) = 12
ord (2) = 6
ord (3) = 4
ord (4) = 3
ord (5) = 12
ord (6) = 2
ord (7) = 12
ord (8) = 3
ord (9) = 4
ord (10) = 6
ord (11) = 12

1.1.13

Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: ...

we've got that

ord (0) = 1
ord (1) = 36
ord (2) = 18
ord (3) = 12
ord (4) = 9
ord (5) = 36
ord (6) = 6
ord (7) = 36
ord (8) = 9
ord (9) = 4
ord (10) = 18
ord (11) = 36
ord (12) = 3
ord (13) = 36
ord (14) = 18
ord (15) = 12
ord (16) = 9
ord (17) = 36
ord (18) = 2

$$\text{ord } (26) = 18$$

$$\text{ord } (35) = 36$$

And since $\overline{-1} = \overline{35}$ and so on, we've got the desired result.

1.1.15

Prove that $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$

We already know that $(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$. Suppose that chain of length $n-1$ has this property. Then we follow that

$$(a_1 \dots a_{n-1} a_n)^{-1} = ((a_1 \dots a_{n-1})(a_n))^{-1} = a_n^{-1} (a_1 \dots a_{n-1})^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$$

thus we follow that if k has this property, then $k+1$ has this property, thus we follow that this property holds for all $n \geq 2$, as desired.

1.1.17

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

We follow that $|x| = n$ means that $x^n = e$, where e denoted identity. Thus

$$e = x^n$$

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

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

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

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

as desired.

1.1.18

Let $x, y \in G$. Prove that $xy = yx$ iff $y^{-1}xy = x$ iff $x^{-1}y^{-1}xy = 1$

$$xy = yx \Leftrightarrow y^{-1}xy = y^{-1}yx \Leftrightarrow y^{-1}xy = ex \Leftrightarrow y^{-1}xy = x \Leftrightarrow x^{-1}y^{-1}xy = x^{-1}x \Leftrightarrow x^{-1}y^{-1}xy = e$$

where $e = 1$, and we've got the reverse implication in \Leftrightarrow by cancelation laws.

1.1.21

Let G be a finite group and let x be an element of G of order n . Prove that if n is odd, then $x = (x^2)^k$.

We follow that $n = 2k - 1$ for some $k \in \mathbb{Z}$, thus

$$\begin{aligned} e &= x^n \\ e &= x^{2k-1} \\ ex &= x^{2k-1}x \\ x &= x^{2k} \\ x &= (x^2)^k \end{aligned}$$

as desired.

1.1.23

Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s, t , prove that $|x^s| = t$

We follow that n is the lowest integer such that

$$x^n = e$$

thus

$$\begin{aligned} x^{st} &= e \\ (x^s)^t &= e \end{aligned}$$

thus t is the smallest integer such that $x^s = e$, therefore $|x^s| = t$, as desired.

1.1.25

Prove that if $x^2 = 1$ for all $x \in G$, then G is abelian.

Suppose that $x, y \in G$. We follow that

$$\begin{aligned} x^2 &= e \\ x^{-1}x^2 &= x^{-1} \\ x &= x^{-1} \end{aligned}$$

by the same logic

$$y = y^{-1}$$

and since $xy \in G$ we've got that

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

thus

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

as desired.

1.1.27

Prove that if x is an element of the group G then $\{x^n : n \in \mathbb{Z}\}$ is a subgroup of G .

Let us denote this set by H and let $y, z, w \in H$. Then we follow that there exist $i, j, k \in \mathbb{Z}$ such that

$$\begin{aligned} y &= x^i \\ z &= x^j \\ w &= x^k \end{aligned}$$

thus

$$yz = x^i x^j = x^{i+j}$$

thus we follow that H is closed under \star . We also have that

$$y(wz) = x^{i+j+k} = (yw)z$$

Since $x^0 = 1$, we follow that $1 \in H$. Also, if $x^n \in H$, then $x^{-n} \in H$, and since $x^n x^{-n} = x^0 = 1$ we follow that every element has an inverse. Thus we conclude that H is indeed a group.

1.1.29

Prove that $A \times B$ is an abelian group iff both A and B are abelian groups.

Let $x, y \in A \times B$. Then we follow that

$$\begin{aligned} xy = yx &\Leftrightarrow (a_x, b_x)(a_y, b_y) = (a_y, b_y)(a_x, b_x) \Leftrightarrow \\ &\Leftrightarrow (a_x a_y, b_x b_y) = (a_y a_x, b_y b_x) \Leftrightarrow a_x a_y = a_y a_x \wedge b_x b_y = b_y b_x \end{aligned}$$

as desired.

1.1.33

Let x be an element of finite order in G .

(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \dots, n-1$.

We follow firstly that

$$x \neq x^2 \neq x^3 \dots \neq x^{n-1}$$

because if we have that $x^i = x^j$ for $1 \leq i < j \leq n-1$, then

$$\begin{aligned} x^i &= x^j \\ x^{-i} x^i &= x^{j-i} \\ 1 &= x^{j-i} \end{aligned}$$

which contradicts that n is the order of x .

Thus we've got that

$$x^i \neq x^{-i}$$

is equivalent to

$$x^{2i} \neq 1$$

If $2i < n$, then we follow that this is given by the fact that order of x is n . If $2i \geq n$, then we follow that $2i < 2n$, therefore $2i - n < n$, and thus

$$x^n x^{2i-n} \neq 1$$

$$x^{2i-n} \neq 1$$

which is given to us by the fact that n is the order of x .

1.2 Dihedral Groups

We firstly state that

$$D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$$

1.2.1

Compute the order of each of the elements in the following groups:

In general, we're going to have that

$$|1| = 1$$

$$|r| = n$$

$$|r^j| = \text{lcm}(j, n)/j$$

$$|s| = |sr^j| = 2$$

(a) D_6

$$|1| = 1$$

$$|r| = 3$$

$$(r^2)^2 = r^4 = rr^3 = r$$

$$(r^2)^3 = r^6 = (r^3)^2 = 1^2 = 1$$

$$|r^2| = 3$$

$$|s| = 2$$

$$(sr)^2 = sr sr = ssr^{-1}r = 1$$

$$|sr| = 2$$

$$(sr^2)^2 = sr^2 sr^2 = srrsrr = sr sr^{-1}rr = ssr^{-1}r^{-1}rr = 1$$

$$|sr^2| = 2$$

(b) D_8

$$|1| = 1$$

$$|r| = 4$$

$$(r^2)^2 = r^4 = 1$$

$$|r^2| = 2$$

$$(r^3)^2 = r^6 = r^2$$

$$(r^3)^3 = r^9 = r$$

$$(r^3)^4 = r^{12} = 1$$

$$|r^3| = 4$$

$$|s| = 2$$

$$|sr| = 2$$

$$srrsrr = sr sr^{-1}rr = ssr^{-1}r^{-1}rr = 1$$

$$|sr^2| = 2$$

$$srrrsrrr = srrsr^{-1}rrr = sr sr^{-1}r^{-1}rrr = ssr^{-3}r^3 = 2$$

$$|sr^3| = 2$$

Not gonna repeat for D_{10} , outlined general case in the beginning of the exercise

1.2.3

Use the generators and relations above to show that every element of D_{2n} , which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr , both of which have order 2.

We follow that

$$rs = sr^{-1}$$

and since $(r^{-1})^{-1} = r$, we follow that

$$r^{-1}s = sr$$

Now suppose that $j \in \mathbb{N}$ such that $sr^j = r^{-j}s$. Then we follow that

$$sr^{j+1} = sr^j r = r^{-j}sr = r^{-j}r^{-1}s = r^{-(j+1)}s$$

thus we conclude that for every $n \in \mathbb{N}$ we've got that $sr^j = r^{-j}s$. Therefore we can follow that

$$(sr^j)^2 = sr^j sr^j = sr^j r^{-j}s = ss = 1$$

therefore $|sr^j| = 2$ for every $j \in \mathbb{Z}$.

Suppose that $x \in D_{2n}$. Then we follow that $x = s^j r^i$ therefore $x = s^{j-i}(sr)^i$, as desired.

1.2.5

If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n} .

Suppose that $x, y \in D_{2n}$. Then we follow that if x is not the identity, then $x = r^j$ or $x = sr^j$. Then we follow that if $x = sr^j$, then

$$xr = sr^{j+1}$$

and

$$rx = r sr^j = sr^{j-1}$$

thus we follow that x does not commute with r^i .

If we let $x = r^j$ then we follow that

$$sx = sr^j$$

and

$$xs = r^j s = sr^{-j} = sr^{n-j}$$

We follow that if n is odd, then there does not exist j such that $j = n - j$, therefore we follow that x does not commute with s .

Thus we can conclude that the only element that commutes with all elements in D_{2n} is the identity, as desired.

1.2.7

Show that $(a, b | a^2 = b^2 = (ab)^n = 1)$ gives a presentation for D_{2n}

Let $a = s$ and $b = sr$. Then we follow that

$$a^2 = s^2 = 1$$

from which we follow that

$$s = s^{-1}$$

$$(ab)^n = s^n s^n r^n = (s^2)^n r^n = 1 r^n = r^n = 1$$

$$b^2 = 1 \Leftrightarrow (sr)^2 = 1 \Leftrightarrow sr = (sr)^{-1} \Leftrightarrow sr = r^{-1} s^{-1} = sr = r^{-1} s$$

thus we conclude that given representation is equivalent to our original representation.

1.2.9

Let G be the group of rigid motions in R^3 of tetrahedron. Show that $|G| = 12$.

We follow that we can send every vertex into another 3 vertices, which gives us 4 motions (don't forget the identity). Then we've got 3 other vertices, with which we can label the second vertex, thus giving us 24 total cases (in general we've got that $|G|$ is equal to number of vertices of the solid multiplied by the number of neighbors of any given vertex.)

1.2.11, 1.2.13

Same logic as in 1.2.9

1.2.15

Find a set of generators and relations for Z/nZ .

1 is the obvious candidate, since $j = \sum 1$ for every $j \in Z/nZ$. We can state that $1^{n+1} = 1$, which will give us a relation. Not sure how to show that this is the extensive list of relations, but here's mine.

1.2.17

Let X_{2n} be a group whose presentation is displayed in (1.2)

$$X_{2n} = \langle x, y | x^n = y^2 = 1, xy = yx^2 \rangle$$

(a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s .

We follow that $1, x, y \in X_{2n}$.

If $z \notin X_{2n}$, then it is represented by $z = x^j y^i$ or $z = y^i x^j$. In former case we can use the relation $y^2 = 1$ to follow that

$$x^j y^i = x^j y$$

from which by induction we can follow that

$$x^j y = y x^{2j}$$

In latter case we follow that $z = y x^j$ or $z = x^j$ by the relation $y^2 = 1$. In any case we follow that

$$z \in X_{2n} \Rightarrow (\exists j \in \mathbb{Z})(z = y x^j \vee z = x^j)$$

Now it would be nice to get that $x^3 = 1$. From the identity in the chapter we follow that

$$x = x^4$$

and therefore $x^3 = 1$, which is neat.

Since $n = 3k$, we follow that

$$x^n = x^{3k} = (x^3)^k = 1$$

thus we follow that $x^n = 1$ does not restrict our set in any way.

Therefore we follow that all the elements of X_{2n} are $1, x, x^2, y, yx, yx^2$, therefore it has order 6, as desired.

Now suppose that we let $x = r$ and $y = s$. Then we follow that we've got relations

$$x^3 = 1$$

$$s^2 = 1$$

$$rs = sr^2 \Leftrightarrow rsr = sr^3 \Leftrightarrow rsr = s \Leftrightarrow sr = r^{-1}s$$

which gives us the desired correspondense

(b) Show that if $(3, n) = 1$, then x satisfies additional relation $x = 1$

We follow that if $(3, n) = 1$, then $3a + qn = 1$, and thus $qn = 1 - 3a$. Thus

$$1 = x^n = x^{qn} = x^n = x^{3a-1} = (x^3)^a x$$

and since $x^3 = 1$ we follow that

$$1 = x^{3a} x = 1x = x$$

from which we follow that the only elements of X_{2n} are $1, y$. Thus $|X_{2n}| = 2$, as desired.