My abstract algebra exercises

Evgeny Markin

2023

Contents

Prelinimaries

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)

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

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)

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

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

0.1.6

Determine whether the function $f : R^+ \to Z$ 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

$$1 = 0.99999999...$$

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

0.1.7

Let $f : A \to B$ 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 $q, w \in Z$ 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 $x_0, y_0 \in Z$ are such that $ax_0 + by_0 = N$. Prove that

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

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + a\frac{b}{d}t + by_0 - b\frac{a}{d}t = ax_0 + by_0 + t(\frac{ab}{d} - \frac{ab}{d}) =$$

$$= ax_0 + by_0 + t(0) = N + 0 = N$$

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
```

```
phi(14) = 6
phi(15) = 8
phi(16) = 8
phi(17) = 16
phi(18) = 6
phi(19) = 18
phi(20) = 8
phi(21) = 12
phi(22) = 10
phi(23) = 22
phi(24) = 8
phi(25) = 20
phi(26) = 12
phi(27) = 18
phi(28) = 12
phi(29) = 28
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 noe 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 numebers 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 of multiples of p in the list $1, 2, ..., n$ 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 $Z/18Z$.

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

0.3.2

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

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

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

$$10a_n \equiv a_n \mod 9$$

and in general

$$10^n a_n \equiv a_n \mod 9$$

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

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

thus

$$8^1 \equiv 8 \mod 29$$

$$8^2 \equiv 6 \mod 29$$

$$8^4 \equiv 36 \equiv 7 \mod 29$$

$$8^8 \equiv 49 \equiv 20 \mod 29$$

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

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

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

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

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

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

0.3.5

$$9^{1500} = ...01$$

0.3.6

Prove that the squares of the elements in $Z/4Z$ *are jsut* 0 *and* 1

We follow that

$$0^2 = 0$$

$$1^2 = 1$$

$$2^2 = 4 \equiv 0 \mod 4$$

$$3^2 = 9 \equiv 1 \mod 4$$

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

$$a^2 \equiv [0, 1] \mod 4$$

$$b^2 \equiv [0, 1] \mod 4$$

thus

$$a^2 + b^2 \equiv [0, 1, 2] \mod 4$$

0.3.8

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

We follow from previous exercise that $a^2 + b^2 \equiv [0, 1, 2] \mod 4$, and $c^2 \equiv [0, 1] \mod 4$, therefore $3c^2 \equiv [0, 3] \mod 4$. Thus we follow that the only possible case is when $a^2 + b^2 \equiv 3c^2 \equiv 0 \mod 4$. Thus we follow all of the a^2, b^2 and c^4 have the factor of 4. Thus there exist a_0, b_0, c_0 such that $a^2 = 4^n a_0^2$, $b^2 = 4^n b_0^2$ $c^2 = 4^n c_0^@$ 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 follow ing 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 clases in Z/nZ is associative

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

1.1.4

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

analogous to previous

1.1.5

Prove that for all $n > 1$ that Z/nZ is not a group under multiplication

We follow that there is no invevrse of $\overline{0}$, Z/nZ 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 $G = \{x \in R : 0 \leq x < 1\}$ 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 $x, y \in R$, and therefore $x + y - \lfloor x + y \rfloor$ is a well-defined on $R \times R \to R$.

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 $1 \leq x + y \leq 2$. 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 $\star : G \times G \to G$ 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

$$(x \star y) \star z =$$

$$= x + y + z - \lfloor y + z \rfloor - \lfloor x + y + z - \lfloor y + z \rfloor \rfloor = x + y + z - \lfloor y + z \rfloor - \lfloor x + y + z \rfloor + \lfloor y + z \rfloor =$$

$$= x + y + z - \lfloor x + y + z \rfloor = x + y + z - \lfloor x + y \rfloor - \lfloor x + y + z \rfloor + \lfloor x + y \rfloor =$$

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

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 indentity 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 $+ : G \times G \to G$. 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 $Z/12Z$.

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 $Z/36Z$: ...

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
```

```
ord (26) = 18
ord (35) = 36
```

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

1.1.15

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

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

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

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 $k \in Z$, thus

$$e = x^n$$
$$e = x^{2k-1}$$
$$ex = x^{2k-1}x$$
$$x = x^{2k}$$
$$x = (x^2)^k$$

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

$$x^{st} = e$$
$$(x^s)^t = e$$

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

$$x^2 = e$$
$$x^{-1}x^2 = x^{-1}$$
$$x = x^{-1}$$

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 $\{x^n : n \in Z\}$ 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 $i, j, k \in Z$ such that

$$y = x^i$$

$$z = x^j$$

$$w = x^k$$

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

$$xy = yx \Leftrightarrow (a_x, b_x)(a_y, b_y) = (a_y, b_y)(a_x, b_x) \Leftrightarrow$$

$$\Leftrightarrow (a_x a_y, b_x b_y) = (a_y a_x, b_y b_x) \Leftrightarrow a_x a_y = a_y a_x \wedge b_x b_y = b_y b_x$$

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 $i = 1, 2, ..., n-1$.

We follow firstly that

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

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

$$x^i = x^j$$

$$x^{-i} x^i = x^{j-i}$$

$$1 = x^{j-i}$$

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 folow 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

$$|1| = 1$$

$$|r| = n$$

$$|r^j| = lcm(j, n)/j$$

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

(a) D_6

$$|1| = 1$$

$$|r| = 3$$

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

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

$$|r^2| = 3$$

$$|s| = 2$$

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

$$|sr| = 2$$

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

$$|sr^2| = 2$$

(b) D_8

$$|1| = 1$$

$$|r| = 4$$

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

$$|r^2| = 2$$

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

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

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

$$|r^3| = 4$$

$$|s| = 2$$

$$|sr| = 2$$

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

$$|sr^2| = 2$$

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

$$|sr^3| = 2$$

Not gonna repeat for D_{10}*, ourlined general case in the beggining 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 $j \in N$ 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 $n \in N$ we've got that $sr^j = r^{-j}s$. Therefore we can follow that

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

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

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 off D_{2n} which commutes with all elements of D_{2n}.

Suppose that $x, y \in D_{2_n}$. 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

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

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_{2_n}

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

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

from which we follow that

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

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

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

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 canditate, 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 replaces by* r *and* y *by* s.

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

If $z \neq\in X_{2n}$, 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

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

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

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

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.

1.3 Symmetric Groups

1.3.1

Let σ and τ be the given permutations. Find the cycle decomposition of their compositions

$$\sigma = (1,3,5)(2,4)$$
$$\tau = (1,5)(2,3)$$
$$\tau\sigma = (1,2,4,3)$$
$$\sigma\tau = (1)(2,5,3,4)$$
$$\tau^2 = (1)(2)(3)(4)(5)$$
$$\tau^2\sigma = (1,3,5)(2,4)$$

1.3.3

For each of the permutations whose cycle decompositions were computed in the preceeding (I've got only one) exercises compute its order

We follow that the general case is the $lcm(l_1, l_2, ...)$, where l_j is the length of j'th cycle

1.3.5

Find the order of $(1,12,8,10,4)(2,13)(5,11,7)(6,9)$.

It's 12.

1.3.7

Write out the cycle decomposition of each element of order 2 *in* S_4.

Skip

1.3.9

(a) Let σ be the 12-cycle $(1,2,3,...,12)$. *For which positive integers i is σ^i also a 12-cycle*

Ones that have $(i,12) = 1$

Rest is similar.

1.3.11

Let σ be the m-cycle $(1,2,...,m)$. *Show taht σ^i is also a ...*

Trivial

1.3.13

Show that an element has order 2 in S_n iff its cycle decomposition is a product of commuting 2-cycles.

We follow that $|S_n| = lcm(l_1, ..., l_n)$, thus if we omit 1-cycles, then S_n has indeed order 2 iff it's a product of commuting 2-cycles.

1.3.15

Prove that the ....

Trivial

1.3.17

Show that if $n \geq 4$, then the number of permutations in S_n which are the product of two disjoint 2-cycles is $n(n-1)(n-2)(n-3)/8$

Let C denote binomial coefficient. We follow that there are $C(n, 2)$ ways to choose the elements in the first cycle, and $C(n-2, 2)$ for the second. Thus there are

$$C(n,2)C(n-2,2) = \frac{n(n-1)}{2}\frac{(n-2)(n-3)}{2} = \frac{n(n-1)(n-2)(n-3)}{4}$$

total elements, if we care about order. Since we don't care about the order of the product, we follow that we can divide this number by $2! = 2$ to get the number of unordered products of disjoint cycles, which will be

$$\frac{n(n-1)(n-2)(n-3)}{8}$$

as desired.

1.3.19

Find all numbers n such that S_7 contains an element of order n

We follow that if element is of order n, then $lcm(l_1, l_2, ..., l_n) = n$. Since $lcm(n, 1, 1, ...) = n$, we follow that all the numbers 1 through n are there. We can also brute-forse this thing and get that $10, 12$ are also present. 9 is out, and so is 8. And that's about it.

1.4 Matrix Groups

1.4.1

Prove that $|GL_2(F_2)| = 6$

We follow that there are only 2 elements in F, therefore there are only 16 matrices in genenral.

We follow that matrices

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

its four rotation,

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

its four rotation and

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

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

are all non-invertible. Every other one is invertible, so we follow that $|GL_2(F_2)| = 6$, as desired.

1.4.3

Show that $GL_2(F_2)$ is non-abelian

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

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

thus we follow that elements in this group do not commute.

1.4.1 1.4.5

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

We can follow that of F is finite, then there are only $|F|^{n^2}$ matrices in total, and invertible matrices are a subset of this set, thus we follow that $GL_n(F)$ is a finite set.

Conversely, suppose that $GL_n(F)$ is a finite group and F is infinite. Then we follow that for every $x \in F$ we've got $xI \in GL_n(F)$, thus we follow that finite set has an infiinte subset, which is a contradiction.

1.4.7

Let p be a prime. Prove that the order of $GL_2(F_p)$ is $p^4 - p^3 - p^2 + p$ There are a total of p^4 distinct matrices. We follow that there are p^2 distinct rows, one of which is zero. If the row is not zero, then it has p distinct scalar multiples. For zero there is p^2 rows, such that one of them is the scalar multiple of the other. Thus we follow that there are

$$(p^2 - 1)p + p^2 = p^3 - p + p^2$$

non-invertible matrices. From this we follow that the total number of invertible matrices is

$$p^4 - p^3 - p^2 + p$$

as desired.

1.4.9

Prove that the binary operation of matrix multiplication of 2×2 matrices with real number entries in associative.

Follows from definition of matrix multiplication, true in general for $n \times n$ matrices.

1.5 Quaternion Group

1.5.1

Compute the order of each of the elements in Q_8

$$|1| = 1$$
$$|-1| = 2$$
$$|i| = 4$$
$$(-i)^2 = (kj)^2 = kjkj = kik = jk = i$$
$$(-i)^3 = (kj)^3 = ikj = (-j)j = 1$$
$$|-i| = 3$$
$$|j| = 4$$
$$(-j)^2 = ikik = ijk = kk = -1$$
$$(-j)^3 = -1(-j) = j$$
$$(-j)^4 = j(-j) = 1$$
$$|-j| = 4$$

$$|k| = 4$$
$$(-k)^2 = jiji = jki = i^2 = -1$$
$$|-k| = 4$$

1.6 Homomorphisms and Isomorphisms

1.6.1

Let $\phi : G \to H$ be a homomorphism

(a) Prove that $\phi(x^n) = \phi(x)^n$

We follow that $\phi(x^2) = \phi(x)^2$ by definition.

Suppose that $\phi(x^n) = \phi(x)^n$. Then we follow that

$$\phi(x^{n+1}) = \phi(x^n x) = \phi(x^n)\phi(x) = \phi(x)^n\phi(x) = \phi(x)^{n+1}$$

thus we follow the desired conclusion from induction.

(b) Do part (a) byt with $n = 1$ and conclude that the same is true for $n \in Z$

We follow that

$$\phi(1x) = \phi(1)\phi(x)$$

and

$$\phi(x1) = \phi(x)\phi(1)$$

thus we can conclude that ϕ maps identity to the identity. Therefore we follow that

$$\phi(x^0) = \phi(1) = 1 = \phi(x)^0$$

$$\phi(x^{-1}) = 1\phi(x^{-1}) = \phi(x)^{-1}\phi(x)\phi(x^{-1}) = \phi(x)^{-1}\phi(xx^{-1}) = \phi(x)^{-1}\phi(1) = \phi(x)^{-1}$$

thus we follow that if $\phi(x^{-1}) = \phi(x)^{-1}$. Suppose now that

$$\phi(x^{-j}) = \phi(x)^{-j}$$

then we follow that

$$\phi(x^{-(j+1)}) = \phi(x^{-j}x^{-1}) = \phi(x^{-j})\phi(x^{-1}) = \phi(x)^{-j}\phi(x)^{-1} = \phi(x)^{-(j+1)}$$

Thus we've got the desired conclusion.

1.6.3

If $\phi : G \to H$ is an isomorphism, prove that G is abelian iff H is abelian. If $\phi : G \to H$ is a homomorphism, what additional conditions on ϕ are sufficient to ensure that if G is abelean, then so H?

Suppose that G is abelian. Now let $x, y \in H$. Because ϕ is a bijection, we follow that it is surjective. Thus we follow that there exist $x', y' \in G$ such that $\phi(x') = x \wedge \phi(y') = y$. Thus we follow that

$$xy = \phi(x')\phi(y') = \phi(x'y') = \phi(y'x') = \phi(y')\phi(x') = yx$$

thus we follow that H is abelian.

If a funtion is a bijection, then the inverse of this function is also surjective. Thus we've got converse case from the forward implication.

If ϕ is a homomorphism, then we follow that if ϕ is surejctive and G is abelian, then H is abelian as well.

1.6.5

Prove that the additive groups R and Q are not isomorphic.

Since there are no bijections from R to Q, we follow that no such functions exist (for the proof GOTO either first chapter of real analysis book, or just google it).

1.6.7

Prove that D_8 and Q_8 are not isomorphic.

Q_8 has an element of order 3, but D_8 does not.

1.6.9

Prove that D_{24} and S_4 are not isomorphic.

We've got that $r^{11} \in D_{24}$ has order 132, and the maximum order of an element in S_4 is below 16 (not gonna compute the exact thing, for more info GOTO 1.3.19)

1.6.11

Let A, B be groups. Prove that $A \times B \cong B \times A$.

Define $\phi((a, b)) = (b, a)$. Then we follow that ϕ is a bijection, and the fact that is a homomorphism is easily followed from definitions.

1.6.13

Let G and H be groups and let $\phi : G \to H$ be a homomorphism. Prove that the image of $\phi, \phi(G)$ is a subgroup of H. Prove that if ϕ is injective, then $G \cong \phi(G)$.

We follow that if $1 \in \phi(G)$, as proven earlier. Associativity comes naturally and inverses are handled in exercise 1.6.1. Thus we follow that $\phi(G)$ is indeded a subgroup.

If ϕ is injective, then we follow that $\phi : G \to \phi(G)$ is a bijection, thus we've got isomorphism, as desired.

1.6.15

Define a map $\pi : R^2 \to R$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π.

Suppose that $x = (a, b), y = (c, d) \in R$. Then we follow that

$$\phi(xy) = \phi(ac, bd) = ac = \phi((a, b))\phi((b, d))$$

therefore ϕ is a homomorphism.

We follow that $(0, y) \in R^2$ is a kernel of π.

1.6.17

Let G be any group. Prove that the map from G to itself, defined by $g \to g^{-1}$ is a homomorphism iff G is abelian.

Suppose that $g \to g^{-1}$ is a homomorphism and let $x, y \in G$. Then we follow that

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

thus we follow that G is abelian.

Suppose that G is abelian. Then we follow that

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

thus we follow that ϕ is a homomorphism.

1.6.19

Let $G = \{z \in C : (\exists n \in Z^+)(z^n = 1)\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \to z^k$ is surjective homomorphism but not an isomorphism.

Suppose that $x, y \in G$. Then we follow that

$$\phi(xy) = (xy)^k = x^k y^k = \phi(x)\phi(k)$$

which proves that ϕ is a homomorphism.

Suppose that $x \in G$. Then we follow that $x =\in C$ and there exists $n \in Z^+$ such that $x^n = 1$. Thus we follow that $x \neq 0$ and we're going to have some x^{-k+1} such that $\phi(x^{-k+1}) = x^1 = x$. We can also follow that $(x^{-k+1})^n = x^n = 1$, thus $x^{-k+1} \in G$. Thus we follow that $x \in \phi(G)$, and therefore ϕ is surjective.

We follow that for every number x in C there exist k elements of C such that

$$x^k = 1$$

. Since $1 \in G$, and $k > 1$ we follow that there exist $x_1 \neq x_2 \in C$ such that

$$\phi(x_1) = 1 = \phi(x_2)$$

thus we follow that ϕ is not injective, and thus it is not an isomorphism.

1.6.21

Prove that for each fixed nonzero $k \in Q$ the map from Q to itself defined by $q \to kq$ is an automorphism of Q.

Assuming that by kq we mean multiplication and letting $\phi(q) = kq$, then we follow that

$$\phi(x + y) = k(x + y) = kx + ky = \phi(x) + \phi(y)$$

thus it is an isomorphism.

We follow that if $x \neq y$, then

$$\phi(x) - \phi(y) = k(x - y) \neq 0$$

thus we follow that $x \neq y$ implies that ϕ is injective.

For $x \in Q$ we follow that $\phi(k^{-1}x) = kk^{-1}x = x$, thus ϕ is also surjective. Thus ϕ is an automorphism.

1.6.23

let G be a finite group which posseses an automorphism σ. such that $\sigma(g) = g$ iff $g = 1$. If σ^2 is the identity map, prove that G is abelian.

Suppose that σ^2 is the identity. We need to show that for all $x, y \in G$ we've got that

$$xy = yx$$

Suppose that $x \in G$. We follow that if $x \neq 1$, then

$$\sigma(x) \neq x$$

but

$$\sigma(x^2) = \sigma(x)^2 = x^2$$

thus we follow that for every $x \in G$, $x^2 = 1$. Thus we follow that $x^{-1} = x$ for every $x \in G$. Therefore we follow that for every $x, y \in G$ we've got that $xy \in G$ as well, thus

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

thus the group is abelian, as desired.

1.6.25

Followes some exercise in my linear algebra book

1.7 Group Actions

1.7.1

Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times$, $a \in F$ and ga is the usual product in F of the two field elemets.

We follow that for all $g_1, g_2, g, a \in F^\times$

$$g_1 \cdot (g_2 \cdot a) = (g_1 \cdot g_2) \cdot a$$

by associative property of multiplication in the field. We also follow that

$$1 \in F$$

by the fact that multiplicative identity is in $F^\times$, and

$$1 \cdot a = a$$

by the fact that 1 is the multiplicative identity.

1.7.3

Shwo that the additive group R acts on the x, y plane $R \times R$ by

$$r \cdot (x, y) = (x + ry, y)$$

We follow that for $r_1, r_2 \in R$ we've got

$$(r_1 + r_2) \cdot (x, y) = (x + r_1y + r_2y, y)$$

$$r_1 \cdot (r_2 \cdot (x, y) = r_1 \cdot (x + r_2y, y) = (x + r_1y + r_2y, y)$$

thus we follow the first part of the definition of group action.

We follow that in this case the group identity in R is 0, therefore for all $(x, y) \in R \cdot R$ is

$$0 \cdot (x, y) = (x + 0y, y) = (x, y)$$

Thus given function satisfies all the properties of group action, and therefore it is a group action itself, as desired.

1.7.5

Prove that the kernel of an action of the group G on the set A is the same as the kernel of corresponding permutation representation $G \to S_A$.

Skip, cannot figure out wording. Kernel of the action is a subset of $G \times A$ and kernel of permutation representation is a subset of G, which means that their sole common subset is $\emptyset$. Kernel of permutation representation may be non-empty, thus we follow that the conclusion of the exercise is false.

1.7.7

Prove that in Example 2 in this section the addition is faithful.

Let $x, y \in F^\times$ be such that $x \neq y$. Let ϕ_1, ϕ_2 be permutations, produced by

$$\phi_1(a) = x \cdot a$$

$$\phi_2(a) = y \cdot a$$

Let $v \in V$ be defined by

$$v = (1, 1, ...)$$

We follow that

$$\phi_1(v) = (x, x, ...)$$

$$\phi_2(v) = (y, y, ...)$$

and since $x \neq y$, we follow that $\phi_1(v) \neq \phi_2(v)$. Thus we follow that $x \neq y$ implies that $\phi_x \neq \phi_y$, as desired.

1.7.8

Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts of the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, ..., a_k\} = \{\sigma(a_1), ..., \sigma(a_k)\}$.

Don't have a clue on why do we need a finite cardinality here, but here we go.

Presumably we define $\cdot : S_A \times B \to B$ to be

$$\cdot(\langle \sigma, b \rangle) = \sigma[b]$$

where [] is defined to be image of B. Since every $\sigma \in S_A$ is a bijection, we follow that for every $b \in B$ there quite literally exists a bijection between b and $\sigma[b]$. Thus we follow that

$$(\forall \sigma \in S_A, b \in B)(|\sigma \cdot b| = |b| = k)$$

(a) Prove that this is a group action.

Suppose that $\sigma_1, \sigma_2 \in S_A$ and $b \in B$ are arbitrary. We follow that

$$\sigma_1 \cdot (\sigma_2 \cdot b) = \sigma_1 \cdot \sigma[b] = \sigma_1[\sigma_2[b]] = (\sigma_1 \cdot \sigma_2)[b]$$

where the last equation quite easily comes from definition of range.

We also follow that if σ is an identity, then

$$\sigma[b] = b$$

by the definition (or minor deriviation and application of definition of range) of identity.

Thus we follow that $\cdot$ is indeed a group action.

Describe explicitly how the elements $(1, 2)$ *and* $(1, 2, 3)$ *act on the six 2-element subsets of* $\{1, 2, 3, 4\}$

We follow that

$$B = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 3\}, \{1, 4\}, \{2, 4\}\}$$

where we're gonna refer to each element of B by b_j, where j is the order of the element in the above-mentioned representation. Then we follow that

$$(1, 2) \cdot b_1 = \{1, 2\}$$

$$(1, 2) \cdot b_2 = \{1, 3\}$$

$$(1, 2) \cdot b_3 = \{3, 4\}$$

$$(1, 2) \cdot b_4 = \{2, 3\}$$

$$(1, 2) \cdot b_5 = \{2, 4\}$$

$$(1, 2) \cdot b_6 = \{1, 4\}$$

$$(1, 2, 3) \cdot b_1 = \{2, 3\}$$

$$(1, 2, 3) \cdot b_2 = \{1, 3\}$$

$$(1, 2, 3) \cdot b_3 = \{1, 4\}$$

$$(1, 2, 3) \cdot b_4 = \{1, 2\}$$

$$(1, 2, 3) \cdot b_5 = \{2, 4\}$$

$$(1, 2, 3) \cdot b_6 = \{3, 4\}$$

1.7.1 1.7.11

Write out the cycle decompositionof the eight permutations in S_4, corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square.

$$()$$
$$(1,2,3,4)$$
$$(1,3)(2,4)$$
$$(1,4,3,2)$$
$$(2,4)$$
$$(1,2)(3,4)$$
$$(1,3)$$
$$(1,4)(2,3)$$

1.7.2 1.7.13

Find the kernel of the left regular action

We follow that the kernel of left regular action is the set

$$A : \{\langle x, y\rangle \in G \times G : x = y^{-1}\}$$

1.7.15

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ do satisfy the axioms of group action of G on itself

Suppose that $x, y, z \in G$. Then we follow that

$$x \cdot (y \cdot z) = x \cdot (zy^{-1}) = zy^{-1}x^{-1}$$

$$(xy) \cdot z = z(xy)^{-1} = zy^{-1}x^{-1}$$

And we follow that

$$1 \cdot z = z1^{-1} = z$$

1.7.17

Let G be a group and let G act on itself by left conjugation (i.e.

$$cdot : G \times G \to G$$

$$g \cdot x = gxg^{-1}$$

)

For $g_1, g_2, a \in G$

$$g_1 \cdot (g_2 \cdot a) = g_1 g_2 a g_2^{-1} g_1^{-1}$$

$$(g_1 g_2) \cdot a = g_1 g_2 a (g_1 g_2)^{-1} = g_1 g_2 a g_2^{-1} g_1^{-1}$$

as desired.

The fact that if we fix g and make a function

$$\sigma_g : G \to G$$

$$\sigma_g(a) = g \cdot a$$

is an automorphism comes from the fact that permutation representation produces permutations (i.e. bijections from G to G), which is precisely the definition of automorrphism.

1.7.3 1.7.18

Let H be a group acting on a set A. Prove that the relation $\equiv$ on A defined by

$$a \equiv b \iff a = hb$$

is an equivalence relation.

We follow that

$$a = 1a \Rightarrow a \equiv a$$

$$a \equiv b \wedge b \equiv c \Rightarrow a = hb \wedge b = h'c \Rightarrow a = hh'c \Rightarrow a \equiv c$$

$$a \equiv b \Rightarrow a = hb \Rightarrow b = h^{-1} a \Rightarrow b \equiv a$$

Chapter 2

Subgroups

2.1 Definition and Examples

Let G be a group

2.1.1 2.1.1

Prove that the specified subset is a subgroup of the given group

Let us denote the desctibed group by H

(a) the set of complex number of the form $a + ai$, $a \in R$ (addition)

$0 = 0 + 0i \in H$, therefore $H \neq \emptyset$. Suppose that $x, y \in H$ $x = a + ai$, $y = b + bi$, then we follow that $y^{-1} = -b - bi \in H$ and

$$xy^{-1} = a + ai - b - bi = (a - b) + (a - b)i \in H$$

therefore we follow that H is a subgroup.

(b) The set of complex numbers of absolute value 1, i.e. the unit circlel in the complex plane (under multiplication)

We follow that $1 \in H$, therefore $H \neq \emptyset$. Suppose that $x, y \in H$. Then we follow that $|y^{-1}| = 1$, therefore $y^{-1} \in H$.

$$|xy^{-1}| = |1| \in H$$

(concrete proof follows from porerties of complex numbers in linear algebra course) therefore H is a subgroup.

(c) For fixed $n \in Z^+$ the set of rational number whose denominators divide n (under addition)

We follow that $1/n \in H$. Suppose that $y \in H$. We follow that $y = m/k$, and thus $y^{-1} = -m/k$, thus $y^{-1} \in H$. Suppose that $x \in H$. We follow that $x = j/l$, and

$$xy^{-1} = s/lcm(l, k)$$

where s is some number and denominator also is a multiple of n, thus H is a subgroup.

(d) rationals whose denominators are relatively prime to n (addition)

If p is prime, then $1/p \in H$. For $y = m/k \in H$, we follow that $y^{-1} = -m/k \in H$, and for some $x = k/l \in H$ we follwo that

$$xy^{-1} = s/lcm(l, k) \in H$$

Thus H is a subgroup

(e) The set of nonzero real number whose square is a rational number (under multiplication)

Here we've got $G = H$.

2.1.2

Prove that subset is not a subgroup

(a) the set of 2*-cycles in* S_n *for* $n \geq 3$.

Suppose that s is defined by $(1, 2)$. We follow that ss^{-1} $(1, 2)(2, 1) = (1)(2)$ which is not a 2-cycle.

(b) The set of reflections in D_{2n} *for* $n \geq 3$.

We follow that $1 \notin H$.

(c) For n *composite integer* > 1 *and* G *is a group containing element of order* n*, the set* $\{x \in G : |x| = n\} \cup \{1\}$.

We follow that if $x \in H$, then $x^n \notin H$

(d) odd integers and 0

$$3 + 3 = 6$$

(e) reals whose square is a rational number (under addition)

$$(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$$

2.1.4

Give an explicit example of a group G *and an infinite subset* H *of* G *is closed under the group operation but is not a subgroup of* G.

Z^+ closed under addition, but does not have inverses.

2.1.5

Prove that G *cannot have a subgroup* H *with* $|H| = n - 1$*, where* $n = |G| > 2$

Suppose that x is the removed element. Then we follow that it cannot be identity by definition of the group. If x is not an identity, then we follow that xy must be removes as well, thus we follow that $|H|$ cannot be $n - 1$.

2.1.6

Let G be an abelian group. Prove that $H = \{g \in G : |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G). Give an explicit example where this set is not a subgroup when G is non-abelian.

We follow that $1 \in H$. Suppose that $y \in H$. We follow that $|y| < \infty$. Thus

$$y^n = 1$$

for some $n \in Z^+$. Thus

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

, therefore $|-y| < \infty$ as well. Suppose that $x \in H$. We follow that there exists $j \in Z^+$ such that

$$x^j = 1$$

thus

$$(xy^{-1})^{lcm(j,n)}) = 1$$

where we can use this fact only because G is abelian, and therefore we can use the fact that

$$(xy)^n = x^n y^n$$

We can have an operator

$$\begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}$$

for which the inverse is

$$\begin{pmatrix} 1 & -0.5 \\ 0 & 0.25 \end{pmatrix}$$

and whose square root is

$$\begin{pmatrix} 1 & 1/3 \\ 0 & 2 \end{pmatrix}$$

where we have that inverse times square root has an infinite order.

2.1.7

Fix some $n \in Z$ with $n > 1$. Find the torsion subgroup of $Z \times (Z/nZ)$. Show taht the set of elements of infinite order together with the identity is not a subgroup of this direct product.

We follow that the only element of Z that has a finite order is 0 and Z/nZ can have $\phi(n)$ (not sure about this, but at least finite) number of elements that have finite order. Thus we follow that the cartesian product of those two sets are the torsion subgroup of $Z \times (Z/nZ)$.

Identity in this case is $\langle 0, 0\rangle$, and we follow that

$$\langle 1, 0\rangle\langle -1, 1\rangle = \langle 0, 1\rangle$$

2.1.8

Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Suppose that $H \cup K$ is a subgroup of G. Let $x \in K \setminus H$ and $y \in H \setminus K$. If $x^{-1} \in H$, then we follow that $(x^{-1})^{-1} \notin H$, therefore H is not closed under inverses. Thus we follow that $x^{-1} \in K \setminus H$. Same applies to y, thus $x, x^{-1} \in K \setminus H$ and $y, y^{-1} \in H \setminus K$.

Now suppose that $xy \in K$. We follow that since $x^{-1} \in K$, then $x^{-1}xy \in K$, therefore $y \in K$, which is a contradiction. Simular case holds for $xy \in H$. Thus we follow that our assumption that $H \setminus K$ and $K \setminus H$ are both nonempty is false. Thus we follow that $H \subseteq K$ or $K \subseteq H$, as desired.

Conversely, if $H \subseteq K$ or $K \subseteq H$, then we follow that $H \cup K = H$ or $H \cup K = K$, thus it's a subgroup.

2.1.9

Let $G = GL_n(F)$ where G is any field. Define

$$SL_n(F) = \{A \in GL_n(F) : det(A) = 1\}$$

Prove that $SL_n(F) \leq GL_n(F)$.

We follow that $I \in SL_n(F)$, thus it is nonempty. Suppose that $x, y \in SL_n(F)$. Then we follow that x, y are both invertible (followed by nonzero determinant), and also $y^{-1} \in SL_n(F)$ (because $\det(A^{-1}) = \det(A)^{-1}$). From this we follow that

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

since $\det(A)\det(B) = \det(AB)$. Thus $SL_n(F) \leq GL_n(F)$, as desired.

2.1.10

Simular case was handled in linear algebra book, gonna skip this one.

2.1.11

Trivial; skip

2.1.12

Let A be an abelian group and fix some $n \in Z$. Prove that the following sets are subgroups of A:

(a) $\{a^n : a \in A\}$

repeat of 1.1.27

(b)

$$H = \{a \in A : a^n = 1\}$$

We follow that $1 \in H$, therefore $H \neq \emptyset$. Suppose that $x, y \in H$. Then we follow that $y^n = 1$. Therefore $y^{-n} = 1$, therefore $y^{\text{-}1} \in H$. Thus we follow that

$$(xy^{\text{-}1})^n = x^n(y^{\text{-}1})^n = 11 = 1$$

2.1.13

Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero $x \in H$. Prove that $H = 0$ or $H = Q$.

We follow that $H = 0$ and $H = Q$ are cases, where everything holds. Now suppose that there exist two nonzero elements x, y of Q such that $x \in H$ and $y' \notin H$. Then we follow that if $y' < 0$, then $y'^{\text{-}1} > 0$ and $y'^{\text{-}1} \notin H \iff y \notin H$, thus we can let $y = \max\{y, y'\}$. (Not gonna remember about it afterwards, this was done so that we've got $x, y > 0$ for simplicity's sake).

Now we get that $x > 0$ and $y > 0$, $x \in H$, $y \notin H$. Since x, y are positive rationals we follow that $x = m/n, y = r/q$ for some $m, n, r, q \in Z^+$.

Since $x \in H$, we follow that every integer multiple of x is in H. Thus we follow that

$$q(m/n) = (qm)/n \in H$$

we can also state by definition of H that

$$n/(qm) \in H$$

therefore every integer multiple of it is also in H. Thus

$$jn/lm \in H$$

for every $j, l \in Z^+$. Thus we follow that

$$(j/l)(n/m) \in H$$

and thus if we set $j/l = (m/n)/(r/q)$ then we can follow that

$$r/q \in H$$

therefore $y \in H$, which is a contradiction. Thus we follow that the only possible cases for H are 0 and Q, as desired.

2.1.14

Show that $H = \{x \in D_{2n} : x^2 = 1\}$ is not a subgroup of D_{2n} (for $n \geq 3$).

We follow that $1, s \in H$. If n is even, then we follow that $r^{n/2}, sr^{n/2} \in H$. We also follow that $sr^j \in H$ for every $j \in Z^+$ since

$$(sr^j)^2 = 1$$

For which we follow that $ssr^j = r^j \in H$, which is a contradiction.

2.1.15

Let $H_1 \leq H_2....$ be an ascending chain of subgroups of G. Prove that

$$\bigcup_{i=1}^{\infty} H_i$$

is a subgroup of G.

Let us denote

$$S = \bigcup_{i=1}^{\infty} H_i$$

Since $1 \in H_1$ and $H_1 \subseteq S$, we follow that $1 \in S$, therefore S is non-empty.

Suppose that $x, y \in S$. Then we follow that $(\exists j, k \in Z^+)(y \in H_j \wedge y \in H_k)$. From this we follow by group property of H_k that

$$(\exists j, k \in Z^+)(y \in H_j \wedge y^{-1} \in H_k)$$

Let $l = \max\{j, k\}$. Then we follow by definition of S that $H_j \subseteq H_l$ and $H_k \subseteq H_l$. Thus

$$(\exists l \in Z^+)(y \in H_l \wedge y^{-1} \in H_l)$$

from which by group property of H_l we follow that

$$(\exists l \in Z^+)(xy^{-1} \in H_l)$$

thus by definition of S we follow that

$$xy^{-1} \in S$$

Thus we conclude that $x, y \in S \Rightarrow xy^{-1} \in S$. Therefore S satisfies all the properties of a subgroup of G. Thus S is a subgroup of G, as desired.

2.1.16

Let $n \in Z^+$ and let F be a field. Prove that the set

$$\{a_{i,j}) \in GL_n(F) : (\forall i > j)(a_{ij} = 0)\}$$

os a subgroup of $GL_n(F)$

Identity is in there and we follow closure under multiplication and inverces by properties in linear algebra book. Same goes for the next exercise as well.

2.2 Centralizers and Normalizers, Stabilizers and Kernels

2.2.1

Prove that $C_G(A) = \{g \in G : (\forall a \in A)(g^{-1}ag = a)\}$.

Suppose that $g' \in C_G(A)$. Since $C_G(A)$ is a group, we follow that there exists $g \in C_G(A)$ such that $g' = g^{-1}$. Thus $g^{-1} \in C_G(A)$. Therefore

$$(\forall a \in A)(g^{-1}a(g^{-1})^{-1} = a) \Leftrightarrow (\forall a \in A)(g^{-1}ag = a)$$

thus $g^{-1} \in \{g \in G : (\forall a \in A)(g^{-1}ag = a)\}$. Therefore $g' \in \{g \in G : (\forall a \in A)(g^{-1}ag = a)\}$.

Suppose that $g' \in \{g \in G : (\forall a \in A)(g^{-1}ag = a)\}$. We follow that

$$(\forall a \in A)(g'^{-1}ag' = a) \Leftrightarrow (\forall a \in A)(ag' = g'a) \Leftrightarrow (\forall a \in A)(a = g'ag'^{-1})$$

thus we follow that $g' \in C_G(A)$. Thus we can follow that $C_G(A) = \{g \in G : (\forall a \in A)(g^{-1}ag = a)\}$ as desired.

2.2.2

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Suppose that $g \in C_G(Z(G))$. We follow that

$$(\forall A \in \mathcal{P}(G) \setminus \{\emptyset\})(g \in C_G(A) \Rightarrow g \in G)$$

and since $Z_G \subseteq G \wedge Z(G) \neq \emptyset$ we follow that $C_G(Z(G)) \subseteq G$.

Suppose that $g \in G$. We follow that

$$(\forall z \in Z(G))(zg = gz)$$

thus

$$(\forall z \in Z(G))(gzg^{-1} = z)$$

thus $g \in C_G(Z(G))$. By double inclusion we get that $C_G(Z(G)) = G$.

Since $C_G(A) \leq N_G(A)$, we follow that $C_G(Z(G)) \leq N_G(Z(G))$. And since both C_G and N_G are subgroups of G, we follow that

$$G \leq C_G(Z(G)) \leq N_G(Z(G)) \leq G$$

thus

$$G = C_G(Z(G)) = N_G(Z(G)) = G$$

as desired.

2.2.3

Prove that if A and B are subsets of G with $A \subseteq B$, then $C_G(B) \leq C_G(A)$

Suppose that $x \in C_G(B)$. We follow that

$$(\forall b \in B)(xbx^{-1} = b)$$

Since $A \subseteq B$, we follow that

$$(\forall a \in A)(xbx^{-1} = a)$$

thus $x \in C_G(A)$. Therefore we conclude that $C_G(B) \subseteq C_G(A)$. And since both are groups, we follow that $C_G(B) \leq C_G(A)$, as desired.

2.2.4

For each of S_3, D_8, Q_8, compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem simplify your work?

Let us firstly state the elements of all of the groups.

S_3 consists of $3! = 6$ permutations in total. Particularly we've got permutations

$$123, 132, 213, 231, 312, 321$$

which produces cycles

$$(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)$$

We can follow that $C_G(1) = G$, by the virtue of the fact that $g1g^{-1} = 1$. Thus we conclude $C_{S_4}[()] = S_4$.

There's a neat program in progs folder (cycles.py) that computes the following result:

```
C_{S_3}[ [(1,), (2,), (3,)] ] = [(1,), (2,), (3,)],
[(1,), (2, 3)], [(1, 2), (3,)], [(1, 2, 3)], [(1, 3, 2)], [(1, 3), (2,)]
C_{S_3}[ [(1,), (2, 3)] ] = [(1,), (2,), (3,)], [(1,), (2, 3)]
C_{S_3}[ [(1, 2), (3,)] ] = [(1,), (2,), (3,)], [(1, 2), (3,)]
C_{S_3}[ [(1, 2, 3)] ] = [(1,), (2,), (3,)], [(1, 2, 3)], [(1, 3, 2)]
C_{S_3}[ [(1, 3, 2)] ] = [(1,), (2,), (3,)], [(1, 2, 3)], [(1, 3, 2)]
C_{S_3}[ [(1, 3), (2,)] ] = [(1,), (2,), (3,)], [(1, 3), (2,)]
```

which seems to deal with the C_{S_3}. Given that the intersection of all of those sets is identity, we follow that $Z(S_3) = \{1\}$

There's a certain result that we can get from here: a centralizer of a subset of a group is an intersection of the centralizers of its elements. We can also follow that $x \in Z(G) \Leftrightarrow C_G(x) = G$ (which is kind of obvious when you think about it for more than a second, but it's still a neat tool).

For D_8 we've got elements $1, r, r^2, r^3, s, sr, sr^2, sr^3$. As in the general case, $C_{D_8}(1) = D_8$. The Lagrange's Theorem in this case implies that the number of elements in the subgroup is either 1, 2, 4 or 8, which simplifies checking a bit. For example, if we know that there are 4 elememnt in the subgroup already, and one element is not in the group, we can conlclude that there are only 4 elements in the subgroup.

$$C_{D_8}(r) = \{1, r, r^2, r^3\}$$

$$C_{D_8}(r^2) = D_8$$

$$C_{D_8}(r^3) = \{1, r, r^2, r^3\}$$

$$C_{D_8}(s) = \{1, s, r^2, sr^2\}$$

$$C_{D_8}(sr) = \{1, sr, r^2, sr^3\}$$

$$C_{D_8}(sr^2) = \{1, r^2, s, sr^2\}$$

$$C_{D_8}(sr^3) = \{1, r^2, sr, sr^3\}$$

From this one we can follow that $Z(D_8) = 1, D_8$

And for Q_8 we've got that cardinalities of possible subgroups are $1, 2, 4$, as in the previous case.

$$C_{Q_8}(1) = Q_8$$

$$C_{Q_8}(-1) = Q_8$$

$$C_{Q_8}(i) = \{1, -1, i, -i\}$$

$$C_{Q_8}(-i) = \{1, -1, i, -i\}$$

$$C_{Q_8}(j) = \{1, -1, j, -j\}$$

$$C_{Q_8}(-j) = \{1, -1, j, -j\}$$

$$C_{Q_8}(k) = \{1, -1, k, -k\}$$

$$C_{Q_8}(-k) = \{1, -1, k, -k\}$$

thus $Z(Q_8) = \{1, -1\}$.

2.2.5

In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ and $A = \{1, (1,2,3), (1,3,2)\}$.

We can follow that

$$C_{S_3}(1) = S_3$$
$$C_{S_3}[(1,2,3)] = \{1, (1,2,3), (1,3,2)\}$$
$$C_{S_3}[(1,3,2)] = \{1, (1,2,3), (1,3,2)\}$$

thus

$$C_{S_3}(A) = \{1, (1,2,3), (1,3,2)\} = A$$

We know that $C_{S_3}(A) \leq N_{S_3}(A) \leq G$. Thus by Lagrange's Theorem we follow that if there exists another element in $N_{S_3}(A)$, then $N_{S_3}(A) = G$. We follow that $(2,3) \circ (1,2,3) \circ (2,3)^{-1} = (1,3,2)$, $(2,3) \circ (1,2,3) \circ (2,3)^{-1} = (1,2,3)$, and $(2,3) \circ 1 \circ (2,3)^{-1} = 1$. Therefore we conclude that $(2,3) \in N_{S_3}(A)$, and thus $N_{S_3}(A) = G$, as desired

(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.

We follow that $C_{D_8}(A) = \{1, r^2, s, sr^2\}$, which we can see by taking appropriate intersections. We can follow that

$$r1r^{-1} = 1$$
$$rr^2r^{-1} = r^2$$
$$rsr^{-1} = sr^2$$
$$rsr^2r^{-1} = s$$

thus we conclude that $N_{D_8}(A) = G$, as desired.

(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4, r^5\}$

Since each element of A is in form r^i for $i \in Z$, we can follow that all of them commute. Thus we follow that $A \subseteq C_{D_{10}}(A)$. From the fact that $sr \neq rs$ and from Lagrange's Theorem we conclude that $C_{D_{10}}(A) = A$. We can also follow that $sr^is = r^{-i}$, thus we conclude that $s \in N_{D_{10}}(A)$. Therefore once again by Lagrange's theorem we follow that $N_{D_{10}}(A) = D_{10}$, as desired.

2.2.6

Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an exapme to show that this is not necessarily true if H is not a subgroup.

Suppose that H is a subgroup of G. Let $h, h' \in H$. We follow that $h^{-1} \in H$, and thus $h^{-1}h' \in H$, therefore $h^{-1}h'h \in H$. Thus we follow that $h(h^{-1}h'h)h^{-1} = h'$. Therefore we follow that for every $h' \in H$ there exists $h^{-1}h'h \in H$ such that $h(h^{-1}h'h)h^{-1} = h'$.

Therefore we conlcude that $hHh^{-1} = H$. Thus we follow that $H \subseteq N_G(H)$. Since H is a group and is a subset of $N_G(H)$ with the same binary operations and whatnot, we follow that $H \leq N_G(H)$, as desired.

Second point is followed from the fact that if H is not a group, then it can't be a subgroup.

(b) Show that $H \leq C_G(H)$ iff H is abelian.

Suppose that $H \leq C_G(H)$. Then we follow that every element of H commutes with every element of H. Thus we follow that H is abelian. Reverse is tirvial as well.

2.2.7

Let $n \in Z$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = 1$ if n is odd.

Suppose that n is odd and $n \geq 3$. Let $x \in D_{2n}$ be such that $x \neq 1$. There are two cases: $x = r^i$ and $x = sr^j$ for $0 < i < n$ and $0 \leq j < n$.

If former is true, then we follow that $sx = sr^j$ and $xs = r^js = sr^{-j} = sr^{n-j}$. Because n is odd, we follow that if j is even, then $n - j$ is odd, thus $xs \neq sx$. If j is odd, then $n - j$ is even, and the same holds. Thus we follow that $r^j \notin Z(D_{2n})$.

If latter is true, then we follow that

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

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

Suppose that $sr^{j+1} = sr^{j-1}$. We follow that $r^{j+1} = r^{j-1}$. If $j = 0$, then $n - 1 \neq 1$ by the fact that $n \geq 3$. If $j = n - 1$, then the same is true. Every other case is also impossible. Thus we have a contradiction and conclude that $sr^j \notin Z(D_{2n})$.

Therefore we follow that $x \neq 1 \Rightarrow x \notin Z(D_{2n})$. Since $1 \in Z(D_{2n})$, we follow that $Z(D_{2n}) = 1$, as desired.

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Dihedral groups (in this book at least) are defined on $n \in Z^+ \wedge n \geq 3$. Thus I think that we're justified to state that $k \in Z^+ \wedge k \geq 2$. Although I'm sure that the definition can be generalized a bit, we're going to assume those conditions for this exercise.

Suppose that $x \notin \{1, r^k\}$. If $x = r^i$ for $1 \leq i < n \wedge i \neq k$, then $r^is = srn - i$ and $sr^i \neq srn - i$ because $i \neq k$. If $x = sr^i$, then the same logic as in the previous section holds. Therefore we follow that $x \notin \{1, r^k\} \Rightarrow x \notin Z(D_{2n})$.

We can follow pretty easily that $\{1, r^k\} \subseteq Z(D_{2n})$. Thus we follow the desired result.

2.2.8

Let $G = S_n$, fix $i \in \{1, 2, ..., n\}$ and let $G_i = \{\sigma \in G : \sigma(i) = i\}$. Use group actions to prove that G_i is a subgroup of G. Find $|G_i|$.

Can't fully figure out what exactly are we supposed to do here. We've already proven through properties of group action, that a stabilizer of an element is a subgroup.

anyways, $|G_i| = (n-1)!$ by simple logic.

2.2.9

For any subgroup H of G and any nonempty subset A of G, define $N_H(A)$ to be the set $\{h \in H : hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H.