



WAYNE STATE  
UNIVERSITY

Algebra I  
Winter 2020

# Contents

<b>1</b>	<b>Integers</b>	<b>3</b>
1.1	Divisors . . . . .	3
1.2	Primes . . . . .	11
<b>2</b>	<b>Functions</b>	<b>26</b>
2.1	Functions . . . . .	26
2.2	Equivalence Relations . . . . .	34
2.3	Permutations . . . . .	35
<b>3</b>	<b>Groups</b>	<b>40</b>
3.1	Definition of a Group . . . . .	40
3.2	Subgroups . . . . .	59
<b>4</b>	<b>Section</b>	<b>84</b>
4.1	A Subsection . . . . .	84
<b>5</b>	<b>Section</b>	<b>85</b>
5.1	A Subsection . . . . .	85
<b>6</b>	<b>Section</b>	<b>86</b>
6.1	A Subsection . . . . .	86
<b>7</b>	<b>Section</b>	<b>87</b>
7.1	A Subsection . . . . .	87
<b>8</b>	<b>Section</b>	<b>88</b>
8.1	A Subsection . . . . .	88
<b>9</b>	<b>Section</b>	<b>89</b>
9.1	A Subsection . . . . .	89
<b>10</b>	<b>Section</b>	<b>90</b>
10.1	A Subsection . . . . .	90

# 1 Integers

## 1.1 Divisors

1. Let  $m, n, r, s \in \mathbb{Z}$ . If  $m^2 + n^2 = r^2 + s^2 = mr + ns$ , prove that  $m = r$  and  $n = s$ .

**Joe Starr**

We select  $m, n, r, s \in \mathbb{Z}$ , given  $m^2 + n^2 = r^2 + s^2 = mr + ns$  which can write as  $m^2 + n^2 - mr - ns = r^2 + s^2 - mr - ns$ . From here we can simplify:

$$\begin{aligned} m^2 + n^2 - mr - ns &= r^2 + s^2 - mr - ns \Rightarrow m(m - r) + n(n - s) = r(r - m) + s(s - n) \\ &\Rightarrow m(m - r) + n(n - s) - r(r - m) - s(s - n) = 0 \\ &\Rightarrow m(m - r) + r(m - r) + n(n - s) + s(n - s) = 0 \\ &\Rightarrow (m - r)(m + r) + (n - s)(n + s) = 0 \end{aligned}$$

from here we can see that in order for  $(m - r)(m + r) + (n - s)(n + s) = 0$  to be true  $m = r$  and  $n = s$ .



5. Use the Euclidean algorithm to find the following greatest common divisors

a (6643, 2873)

b (7684, 4148)

c (26460, 12600)

d (6540, 1206)

e (12091, 8439)

**Joe Starr**

(a) (6643, 2873)

$$6643 = 2873 * 2 + 897$$

$$2873 = 897 * 3 + 182$$

$$897 = 182 * 4 + 169$$

$$182 = 169 * 1 + 13$$

$$169 = 13 * 13$$

(b) (7684, 4148)

$$7684 = 4148 * 1 + 3536$$

$$4148 = 3536 * 1 + 612$$

$$3536 = 612 * 5 + 476$$

$$612 = 476 * 1 + 136$$

$$476 = 136 * 3 + 68$$

$$136 = 68 * 2$$

(c) (26460, 12600)

$$26460 = 12600 * 2 + 1260$$

$$12600 = 1260 * 10$$

(d) (6540, 1206)

$$6540 = 1206 * 5 + 510$$

$$1206 = 510 * 2 + 186$$

$$510 = 186 * 2 + 138$$

$$186 = 138 * 1 + 48$$

$$138 = 48 * 2 + 42$$

$$48 = 42 * 1 + 6$$

$$42 = 6 * 7$$

(e) (12091, 8439)

$$12091 = 8439 * 1 + 3652$$

$$8439 = 3652 * 2 + 1135$$

$$3652 = 1135 * 3 + 247$$

$$1135 = 247 * 4 + 147$$

$$247 = 147 * 1 + 100$$

$$147 = 100 * 1 + 47$$

$$100 = 47 * 2 + 6$$

$$47 = 6 * 7 + 5$$

$$6 = 5 * 1 + 1$$

$$5 = 1 * 5$$

7. For each part of Exercise 5, find integers  $m$  and  $n$  such that  $(a, b)$  is expressed in the form  $ma + nb$ .

**Joe Starr**

(a)  $(6643, 2873)$

$$(6643) - 16 + (2873) 37 = 13$$

(b)  $(7684, 4148)$

$$(7684) 27 + (4148) - 50 = 68$$

(c)  $(26460, 12600)$   $(26460) 1 + (12600) - 2 = 1260$

(d)  $(6540, 1206)$   $(6540) - 26 + (1206) 141 = 6$

(e)  $(12091, 8439)$   $(12091) 1435 + (8439) - 2056 = 1$

9. let  $a, b, c$  be integers such that  $a + b + c = 0$ . Show that if  $n$  is an integer which is a divisor of two of the three integers, then it is also a divisor of the third.

**Joe Starr**

Select  $a, b, c \in \mathbb{Z}$  to satisfy  $a + b + c = 0$ , WLOG let  $n \in \mathbb{Z}$  such that  $n|a$  and  $n|b$ . Since  $(a + b) + c = 0$  it must be that  $(a + b) = -c$ . From here we must show  $n|(a + b)$ , or  $a + b = nq$ . Since  $n|a$  and  $n|b$  we may write  $a = nq_1$  and  $b = nq_2$ , yielding,  $nq_1 + nq_2 = n(q_1 + q_2) = nq$  thus  $n|c$ , as desired.  $\square$

13. Show that if  $n$  is any integer, then  $(10n+3, 5n+2) = 1$

**Joe Starr**

We begin with the Euclidean algorithm,

$$10n + 3 = (5n + 2) 1 + (5n + 1)$$

$$5n + 2 = (5n + 1) 1 + 1$$

from here we have  $(10n + 3, 5n + 2) = (5n + 2, 5n + 1) = 1$ , as desired.



15. For what positive integers  $n$  is it true that  $(n, n + 2) = 2$ ? Prove your claim.

**Joe Starr**

The conjecture is that the statement is true for even values of  $n$ . We begin with rewriting  $n$  in terms of  $k$ ,  $n = 2k$  the Euclidean algorithm,

$$\begin{aligned}(2k) + 2 &= (2k) 1 + (2) \\ 2k &= (2) k\end{aligned}$$

from here we have  $(n + 2, n) = (2k + 2, 2k) = 2$ , as desired.

17. Show that the positive integer  $k$  is the difference of two odd squares if and only if  $k$  is divisible by 8.

**Joe Starr**

We begin by writing  $k = a^2 - b^2$ , since  $a$  and  $b$  are odd we can write,

$$a = 2r + 1$$

$$b = 2s + 1$$

from here we have  $a^2 - b^2 = 4(r + s + 1)(r - s)$ . Since  $k > 0$  we must consider two cases  $r - s = 2m + 1$  and  $r - s = 2m$ .

$r - s = 2m$ :

In this case we have  $a^2 - b^2 = 4(r + s + 1)2m = 8(r + s + 1)m$  and we are done.

$r - s = 2m + 1$ :

In this case we have  $r - s = 2m + 1$  and  $r + s = r - s + 2s = 2m + 1 + 2s$

$$\begin{aligned} a^2 - b^2 &= 4(r + s + 1)(2m + 1) \\ &= 4(2m(r + s + 1) + (r + s + 1)) \\ &= 4((2mr + 2ms + 2m) + (r + s + 1)) \\ &= 4(2mr + 2ms + 2m + r + s + 1) \\ &= 4(2mr + 2ms + 2m + 2m + 1 + 2s + 1) \\ &= 4(2mr + 2ms + 2m + 2m + 2s + 2) \\ &= 8(mr + ms + m + m + s + 1) \end{aligned}$$

as desired.

## 1.2 Primes

1. Find the prime factorizations of each of the following numbers, and use them to compute the greatest common divisor and least common multiple of the given pairs of numbers.

(a) (35, 14)

(c) (252, 11)

(e) (6643, 2873)

(b) (15, 11)

(d) (7684, 4148)

### Joe Starr

(a) (35, 14)  
35 : 5, 7

14 : 2, 7  
gcd: 7  
lcm: 70

(b) (15, 11)  
15 : 3, 5

11 : 11  
gcd: 1  
lcm: 165

(c) (252, 180)  
252 : 2, 2, 3, 3, 7

180 : 2, 2, 3, 3, 5  
gcd: 36  
lcm: 1260

(d) (7684, 4148)  
7684 : 2, 2, 17, 113

4148 : 2, 2, 17, 61  
gcd: 68  
lcm: 468724

(e) (6643, 2873)  
6643 : 7, 13, 73

2873 : 13, 13, 17  
gcd: 13  
lcm: 1468103

2. Use the sieve of Eratosthenes to find all prime numbers less than 200.

Joe Starr

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

3. For each composite number  $a$ , with  $4 \leq a \leq 20$ , find all positive numbers less than  $a$  that are relatively prime to  $a$ .

**Joe Starr**

4 : 2, 3

6 : 2, 3, 5

8 : 2, 3, 5, 7

9 : 2, 3, 4, 5, 7, 8

10 : 2, 3, 5, 7, 9

12 : 2, 3, 5, 7, 11

14 : 2, 3, 5, 7, 9, 11, 13

15 : 2, 3, 4, 5, 7, 8, 11, 13, 14

16 : 2, 3, 5, 7, 9, 11, 13, 15

18 : 2, 3, 5, 7, 11, 13, 17

20 : 2, 3, 5, 7, 9, 11, 13, 17, 19

4. Find all positive integers less than 60 and relatively prime to 60.

**Joe Starr**

60 : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59

9. (a) For which  $n \in \mathbb{Z}^+$  is  $n^3 - 1$  a prime number?
- (b) For which  $n \in \mathbb{Z}^+$  is  $n^3 + 1$  a prime number?
- (c) For which  $n \in \mathbb{Z}^+$  is  $n^2 - 1$  a prime number?
- (d) For which  $n \in \mathbb{Z}^+$  is  $n^2 + 1$  a prime number?

**Joe Starr**

- (a) We can factor  $n^3 - 1$  into  $(n - 1)(n^2 + n + 1)$ . We have then  $n - 1 | n^3 - 1$ , for  $n^3 - 1$  to be prime  $n - 1$  must be 1. This happens only for  $n = 2$ .
- (b) We can factor  $n^3 + 1$  into  $(n + 1)(n^2 - n + 1)$ . We have then  $(n^2 - n + 1) | n^3 + 1$ , for  $n^3 + 1$  to be prime  $(n^2 - n + 1)$  must be 1. This happens only for  $n = 1$ .
- (c) We can factor  $n^2 - 1$  into  $(n - 1)(n + 1)$ . We have then  $(n + 1) | n^2 - 1$ , for  $n^2 - 1$  to be prime  $(n - 1)$  must be 1. This happens only for  $n = 2$ . For which  $n \in \mathbb{Z}^+$  is  $n^2 - 1$  a prime number?
- (d) ????

11. Prove that  $n^4 + 4^n$  is composite if  $n > 1$ .

**Joe Starr**

We are presented with two potability's,  $n$  is even or  $n$  is odd.

$n$  even

It's obvious that  $n^4 + 4^n$  is an even not 2 and can't be prime.

$n$  odd

We begin by completing the square

$$\begin{aligned}n^4 + 4^n &= n^4 + 4^n \\&= (n^2)^2 + (2^n)^2 \\&= (n^2 + 2^n)^2 - 2n^2 2^n\end{aligned}$$

We from here we observe that  $2^n 2 = 2^{n+1}$ , since  $n$  is odd  $n + 1$  is even yielding  $2^{n+1} = 2^{2k}$ . We can see we have a difference of squares

$$\begin{aligned}(n^2 + 2^n)^2 - 2n^2 2^n &= (n^2 + 2^n)^2 - (2^n n)^2 \\&= (n^2 + 2^n + 2^n n) (n^2 + 2^n - 2^n n)\end{aligned}$$

since we are restricted to  $n > 1$  we can see that both  $(n^2 + 2^n + 2^n n) > 1$  and  $(n^2 + 2^n - 2^n n) > 1$  for all  $n$ . Making  $n^4 + 4^n$  composite as desired.



13. Let  $a, b, c$  be positive integers, and let  $d = (a, b)$ . Since  $d|a$ , there exists an integer  $h$  with  $a = dh$ . Show that  $a|bc$ , then  $h|c$ .

**Joe Starr**

We will proceed with a transitive proof:

$$\begin{aligned} a|abc &\rightarrow a|(a, b) c \\ &\rightarrow a|dc \\ &\rightarrow dh|dc \\ &\rightarrow h|c \end{aligned}$$

14. Show that  $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]$ .

**Joe Starr**

Let  $x \in (a\mathbb{Z} \cap b\mathbb{Z})$ , since  $x \in a\mathbb{Z}$  we have  $x = aq_1$ , similarly since  $x \in b\mathbb{Z}$  we have  $x = bq_2$ . We can see that  $x = abq$ , this means  $x$  is a multiple of  $[a, b]$  putting  $x \in [a, b]$ . Next, we let  $x \in [a, b] \mathbb{Z}$ , this means  $x$  is of the form  $x = [a, b] q$ . We can see that  $a|x$  and  $b|x$  since  $a|[a, b]$ , This makes  $x \in a\mathbb{Z}$  and  $x \in b\mathbb{Z}$ , as desired.

17. Let  $a, b$  be nonzero integers. Prove  $(a, b) = 1$  if and only if  $(a + b, ab) = 1$ .

**Joe Starr**

$\Rightarrow$  We let  $(a, b) = 1$ , then consider the  $(a + b, ab)$ . We assume  $(a + b, ab) = d$ , with  $d > 1$ . Since  $d > 1$  there must exist  $p$  a prime such that  $p|d$ . This means that  $p|a + b$  and  $p|ab$ . Consequently, either  $p|a$  or  $p|b$ . WOLOG we have  $p|a$ , and since  $p|a + b$  it must be that  $p|b$ . Finally, since  $p|a$  and  $p|b$ ,  $p|(a, b)$  a contradiction. So  $(a + b, ab) = 1$ .

$\Leftarrow$  We let  $(a + b, ab) = 1$ , then consider the  $(a, b)$ . We assume  $(a, b) = d$ , with  $d > 1$ . Since  $d > 1$  there must exist  $p$  a prime such that  $p|d$ . This means that  $p|a$  and  $p|b$ , further  $p|ab$ . Since  $p$  divides  $a$  and  $b$ , we have  $p|a + b$ . Finally, since  $p|ab$ , and  $p|a + b$ ,  $p|(a + b, ab)$ , a contradiction so  $(a, b) = 1$ .

18. Let  $a, b$  be nonzero integers with  $(a, b) = 1$ . Compute  $(a + b, a - b)$ .

**Joe Starr**

We know that  $d = (a + b, a - b)$ , this means that  $d|a + b$  and  $d|a - b$ . From here we have that  $d|(a + b) + (a - b) \rightarrow d|2a$  and  $d|(a + b) - (a - b) \rightarrow d|2b$ . Since  $d$  divides both  $2a$  and  $2b$ ,  $d$  must also divide  $2(a, b)$ . Since  $(a, b) = 1$  we have  $(a + b, a - b) = 2$ .

19. Let  $a$  and  $b$  be positive integers, and let  $m$  be an integer such that  $ab = m(a, b)$ . Without using the prime factorization theorem, prove that  $(a, b)[a, b] = ab$  by verifying that  $m$  satisfies the necessary properties of  $[a, b]$ .

**Joe Starr**

We let  $d = (a, b)$ , this means that  $ab = md$ . We first show  $a|m$  and  $b|m$ ,

$$\begin{aligned} ab = md &\rightarrow a(dq) = md \\ &\rightarrow adq - md = 0 \\ &\rightarrow d(aq - m) = 0 && (by\ d \neq 0) \\ &\rightarrow aq = m \\ &\rightarrow a|m \end{aligned}$$

similarly for  $b$ .

Next we will show that if  $a|c$  and  $b|c$  then  $m|c$ . We have that  $c = aq_1 = bq_2$  or  $c^2 = abq$ . We can multiply  $ab = md$  by  $q$  giving  $abq = mdq$ , this means we have  $c^2 = mdq$ , which is true only if  $c = mdq$ ,  $m|c$  as desired.

20. A positive integer  $a$  is called a square if  $a = n^2$  for some  $n \in \mathbb{Z}$ . Show that the integer  $a > 1$  is a square if and only if every exponent in its prime factorization is even.

**Joe Starr**

Let  $a \in \mathbb{Z}$  be a square. Since  $a$  is a square by definition there exists a  $n$  such that  $nn = a$ . Now by the fundamental theorem of arithmetic we know  $n$  has a prime factorization, written  $p_1^{n_1} \cdots p_k^{n_k}$ . If we consider  $nn$ , we have  $nn = (p_1^{n_1} \cdots p_k^{n_k})(p_1^{n_1} \cdots p_k^{n_k})$ , by combining terms we can see that  $nn = (p_1^{2n_1} \cdots p_k^{2n_k})$ , as desired.

23. Let  $p$  and  $q$  be prime numbers. Prove that  $pq + 1$  is a square if and only if  $p$  and  $q$  are twin primes.

**Joe Starr**

We begin by letting selecting  $p$  a prime and  $q$  a prime such that  $q = p + 2$ . Now we consider  $pq$ ,

$$\begin{aligned}pq &\rightarrow p(p + 2) \\ &\rightarrow p^2 + p2\end{aligned}$$

We now consider  $p + 1$ , if we take  $(p + 1)^2$ , we get  $p^2 + 2p + 1$ . It's obvious that  $pq + 1 = p^2 + p2 + 1 = (p + 1)^2$ , so  $pq + 1$  is a square when  $p$  and  $q$  are twin primes. We can now consider  $p$  a prime, and  $q$  a prime such that  $q = p + n$  with  $n > 2$ . If we calculate  $pq$  we see that,

$$\begin{aligned}pq &\rightarrow p(p + n) \\ &\rightarrow p^2 + pn\end{aligned}$$

we then have that  $pq + 1 = p^2 + pn + 1$  with  $n > 2$ , this is not a square, showing when  $p$  and  $q$  aren't twin primes  $pq + 1$  is not a square.

26. Prove that if  $a > 1$ , then there is a prime  $p$  with  $a < p \leq a! + 1$ .

**Joe Starr**

We observe that  $a! + 1$  is either prime or composite, if  $a! + 1$  is prime we are done, if  $a! + 1$  is composite we know by the fundamental theorem of arithmetic that  $a! + 1$  has prime factors. Now if all prime factors  $p$  are such that  $p \leq a$  since  $p|a!$  we see that if we divide  $a! + 1$  by any of these we get a remainder of 1, a contradiction so there must be a prime factor  $p$  with  $a < p$ .

*Note: this is basically the same argument as euclid's proof of infinite primes*



29. Show that  $\log 2 / \log 3$  is not a rational number.

**Joe Starr**

We observe this is an application of the change of base formula, making  $\frac{\log 2}{\log 3} = \log_3 2$ . From here we have  $x = \log_3 2 \rightarrow 3^x = 2$ , if  $x$  is rational then there exist  $m$  and  $n$  such that  $\frac{m}{n} = x$ . We now have  $3^{\frac{m}{n}} = 2 \rightarrow 3^m = 2^n$ , a contradiction since there is no  $m$  and  $n$  that satisfy this equivalence, making  $\log 2 / \log 3$  irrational as desired.

## 2 Functions

### 2.1 Functions

1. In each of the following parts, determine whether the given function is 1:1 and whether it is onto.

(a)  $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = x + 3$

(b)  $f : \mathbb{C} \rightarrow \mathbb{C}; f(x) = x^2 + 2x + 1$

(c)  $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n; f([x]_n) = [mx + b]_n$ , where  $m, b \in \mathbb{Z}$

(d)  $f : \mathbb{R}^+ \rightarrow \mathbb{R}; f(x) = \ln x$

#### Joe Starr

(a) We can see that  $f(x) = x + 3$  then  $f^{-1}(x) = x - 3$ ,  $f(f^{-1}(x)) = (x - 3) + 3 = x$ . Showing  $f$  is a bijection.

(b) 1:1:

Assume  $f(x) = 25 = f(y)$ , we can see that if  $x = 4$ ,  $f(x) = 25$ , and  $y = -6$ ,  $f(y) = 25$ , showing  $f$  not injective.

onto:

Let  $y \in \mathbb{C}$  we must now show there exists a  $x \in \mathbb{C}$  such that  $f(x) = y$ . Consider  $x = \sqrt{y} - 1$ , we can then take:

$$\begin{aligned} f(x) &= x^2 + 2x + 1 \\ &= (\sqrt{y} - 1)^2 + 2(\sqrt{y} - 1) + 1 \\ &= (\sqrt{y} - 1)^2 + 2\sqrt{y} - 2 + 1 \\ &= 1 - 2\sqrt{y} + y + 2\sqrt{y} - 1 \\ &= y \end{aligned}$$

showing  $f$  surjective.

(c) Consider  $f^{-1}(x) = [(y - b)m^{-1}]_n$ , now taking  $f(f^{-1}(x))$

$$\begin{aligned} f(f^{-1}(x)) &= [m(x - b)m^{-1} + b]_n \\ &= [(x - b) + b]_n \\ &= [x]_n \end{aligned}$$

showing  $f$  a bijection.





4. For each 1:1 and onto function in Exercise 2, find the inverse of the function

(a)  $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = x^2$

(b)  $f : \mathbb{C} \rightarrow \mathbb{C}; f(x) = x^2$

(c)  $f : \mathbb{R}^+ \rightarrow \mathbb{R}^+; f(x) = x^2$

(d)  $f : \mathbb{R}^+ \rightarrow \mathbb{R}^+; f(x) = \begin{cases} x & \text{if } x \text{ is rational} \\ x^2 & \text{if } x \text{ is irrational} \end{cases}$

**Joe Starr**

(a) Not a bijection

(b) Not a bijection

(c)  $f^{-1}(x) = +\sqrt{x}$

(d)  $f : \mathbb{R}^+ \rightarrow \mathbb{R}^+; f^{-1}(x) = \begin{cases} x & \text{if } x \text{ is rational} \\ +\sqrt{x} & \text{if } x \text{ is irrational} \end{cases}$

13. Let  $f : A \rightarrow B$  be a function, and let  $f(A) = \{f(a) \mid a \in A\}$  be the image of  $f$ . Show that  $f$  is onto if and only if  $f(A) = B$ .

**Joe Starr**

Let  $f(A) = B$ , select  $y \in B$ , since  $y \in B$  we have  $y \in f(A)$ , that means there exists  $a \in A$  such that  $f(a) = y$ . Showing  $f$  surjective. Let  $f(A) \neq B$ , let  $y \in B$ , such that  $y \notin B \cap f(A)$ . Since we have  $y \notin f(A)$  we have no  $a \in A$  that maps to  $y$  showing  $f$  not surjective, as desired.

15. Let  $f : A \rightarrow B$  and  $g : B \rightarrow C$  be functions. Prove that if  $g \circ f$  is 1:1, then  $f$  is 1:1, and that if  $g \circ f$  is onto  $g$  is onto.

**Joe Starr**

Let  $g \circ f$  be injective, but  $f$  not injective. Since  $f$  is not injective  $\exists a, x \in A$  such that  $a \neq x$  but  $f(x) = f(a)$ . We consider  $g \circ f(a)$  and  $g \circ f(x)$ , since  $f(x) = f(a)$  it must be that  $g(f(x)) = g(f(a))$ . This means that with  $a \neq x$ ,  $g(f(x)) = g(f(a))$ , making  $g \circ f$  not injective a contradiction so  $f$  injective.

Let  $g \circ f$  be surjective, but  $g$  not surjective. Since  $g$  not surjective there exists some  $c \in C$  such that  $g(b) \neq c$  for all  $b \in B$ . However since  $g \circ f$  surjective there exists  $g \circ f(a) = c$  a contradiction, making  $g$  surjective.

17. Let  $f : A \rightarrow B$  be a function. Prove that  $f$  is onto if and only if  $h \circ f = k \circ f$  implies  $h = k$ , for every set  $C$  and all choices of functions  $h : B \rightarrow C$  and  $k : B \rightarrow C$ .

**Joe Starr**

Assume  $f$  is surjective, that is for all  $y \in B$  there exists  $x \in A$  such that  $f(x) = y$ . We know  $h(f(x)) = k(f(x))$ , so  $h(y) = k(y)$  for all  $y$  in the domain of  $f$  as desired.

Next assume  $f$  is not surjective, then for some  $y \in B$  there exists no  $x$  such that  $f(x) = y$ . We can select  $C = \{a, b\}$ . We say that  $h(c) = a$  now we construct  $k$ ,

$$k(x) = \begin{cases} b & \text{if } x = y \\ a & \text{if } x \neq y \end{cases}$$

from here we have that when the input of  $h$  and  $k$  are in the domain of  $f$   $h \neq k$ , as desired.



19. Let  $f : A \rightarrow B$  be a function. Prove that  $f$  is 1:1 if and only if  $f \circ h = f \circ k$  implies  $h = k$ , for every set  $C$  and all choices of functions  $h : C \rightarrow A$  and  $k : C \rightarrow A$ .

**Joe Starr**

Assume that  $f$  is injective, this means that  $f(x) = f(y)$  implies  $x = y$ . Also assume  $f \circ h = f \circ k$  for some  $h, k$ . We assume  $h \neq k$  for some  $c \in C$ . Since we know  $f$  is injective we have  $f(h(c)) \neq f(k(c))$ , a contradiction from our assumption that  $f \circ h = f \circ k$  meaning  $h = k$  as desired.

Assume  $f \circ h = f \circ k$  implies  $h = k$ . suppose  $f$  be not injective, this means that there exists some  $x, y$  such that  $f(x) = f(y)$  but  $x \neq y$ . We can select  $C = \{a, b\}$ , and define  $h, k$ :

$$\begin{array}{ll} k(a) = x & h(a) = y \\ k(b) = y & h(b) = x \end{array}$$

We can see from here we have that for  $f(h(a)) = f(k(a))$  but  $h \neq k$  a contradiction making  $f$  injective as desired.

## 2.2 Equivalence Relations

## 2.3 Permutations

1. Consider the following Permutations in  $S_7$ .

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 7 & 4 & 6 & 3 \end{pmatrix}$$

(a) $\sigma\tau$		(c) $\tau^2\sigma$		(e) $\sigma\tau\sigma^{-1}$	
(b) $\tau\sigma$		(d) $\sigma^{-1}$		(f) $\tau^{-1}\sigma\tau$	

**Joe Starr**

$$(a) \quad \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 7 & 4 & 1 & 5 \end{pmatrix}$$

$$(b) \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 4 & 7 & 6 & 2 & 3 \end{pmatrix}$$

$$(c) \quad \tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 3 & 6 & 1 & 5 \end{pmatrix}$$

$$(d) \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 4 & 3 & 5 & 7 \end{pmatrix}$$

$$(e) \quad \sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 7 & 6 & 4 & 5 \end{pmatrix}$$

$$(f) \quad \tau^{-1}\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 6 & 1 & 7 \end{pmatrix}$$

2. Write each of the permutations  $\sigma\tau, \tau\sigma, \tau^2\sigma, \sigma^{-1}, \sigma\tau\sigma^{-1}$ , and  $\tau^{-1}\sigma\tau$  in Exercise 1 as a product of disjoint cycles. Write  $\sigma$  and  $\tau$  as products of transpositions.

**Joe Starr**

(a)  $\sigma\tau = (1236)(475)$

(b)  $\tau\sigma = (1562)(347)$

(c)  $\tau^2\sigma = (143756)$

(d)  $\sigma^{-1} = (1653)$

(e)  $\sigma\tau\sigma^{-1} = (23)(4756)$

(f)  $\tau^{-1}\sigma\tau = (1356)$

( $\sigma$ )  $\sigma = (13)(35)(56)$

( $\tau$ )  $\tau = (12)(35)(54)(47)(73)$

3. Write  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 10 & 5 & 7 & 8 & 2 & 6 & 9 & 1 \end{pmatrix}$  as the product of disjoint cycles and as a product of transpositions. Construct its associated diagram, find its inverse, and find its order.

**Joe Starr**

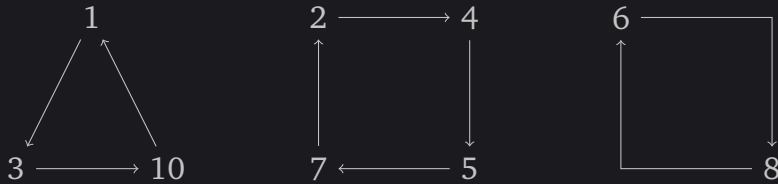
Disjoint cycles:

$$(1, 3, 10) (2, 4, 5, 7) (6, 8)$$

Transpositions:

$$(1, 3) (3, 10) (2, 4) (4, 5) (5, 7) (6, 8)$$

Diagrams:



Inverse:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 1 & 2 & 4 & 8 & 5 & 6 & 9 & 3 \end{pmatrix}$$

Order:

$$(1, 3, 10) = 3, (2, 4, 5, 7) = 4, (6, 8) = 2 \text{ order is } 12$$



5. Let  $3 \leq m \leq n$ . Calculate  $\sigma\tau^{-1}$  for cycles  $\sigma = (1, 2, \dots, m-1)$  and  $\tau = (1, 2, \dots, m-1, m)$  in  $S_n$ .

**Joe Starr**

We begin with finding  $\tau^{-1}$ . We take  $\tau$  of,  $[1, 2, \dots, m-1, m]$ , we get  $[2, 3, \dots, m, 1]$ . If we now apply  $\tau^{-1} = (m, 1, 2, \dots, m-1)$ , we get  $[1, 2, \dots, m-1, m]$ .

We can now compose  $\tau^{-1}$  and  $\sigma$  yielding  $(m, m-1, 1, 2, \dots, m-3, m-2)$ .

## 3 Groups

### 3.1 Definition of a Group

1. Using ordinary addition of integers as the operation, show that the set of even integers is a group but the set of odd integers is not.

#### Joe Starr

We begin considering the even integers, that is integers of the form  $2k$ . We must also include 0 in the even integers. We get the identity element as well as Associativity and inverses for free from integer addition on  $\mathbb{Z}$ . We then consider closure. Let  $n$  and  $m$  be even integers, if we take  $m + n$  we can see we have,  $m + n = 2k_m + 2k_n = 2(k_m + k_n)$  an even integer. Making the even integers a group under addition.

Next we consider the odd integers, take  $3 + 3 = 2(3)$  an even integer, showing odds are not closed under addition and not a group.



2. For each binary operation  $*$  defined on a set below, determine whether or not  $*$  gives a group structure on the set. If it is not a group, say which axioms fail to hold.

(a) Define  $*$  on  $\mathbb{Z}$  by  $a * b = ab$ .

(b) Define  $*$  on  $\mathbb{Z}$  by  $a * b = \max a, b$ .

(c) Define  $*$  on  $\mathbb{Z}$  by  $a * b = a - b$ .

(d) Define  $*$  on  $\mathbb{Z}$  by  $a * b = |ab|$ .

(e) Define  $*$  on  $\mathbb{R}^+$  by  $a * b = ab$ .

(f) Define  $*$  on  $\mathbb{Q}$  by  $a * b = ab$ .

### Joe Starr

(a) Inverses: Let  $a \in \mathbb{Z}$  but  $a \neq 1$  and  $a \neq -1$ ,  $a^{-1} \notin \mathbb{Z}$ .

(b) Identity:  $\max a, a - 1 = a$  for all  $a \in \mathbb{Z}$  this means there is no  $e$  with  $\max a, e = a$  for all  $a$ .

(c) Associativity:

$$\begin{aligned}(a * b) * c &= (a - b) * c \\ &= (a - b) - c \\ &= a - (b + c) \\ &= a * (b + c)\end{aligned}$$

Inverses: Select  $a \in \mathbb{Z}$ ,

$$a * a = a - a = 0$$

Closure: Obvious from closure of  $(\mathbb{Z}, +)$

Identity: 0 is the identity, Obvious from  $(\mathbb{Z}, +)$

(d) Inverses: Let  $a \in \mathbb{Z}$  but  $a \neq 1$  and  $a \neq -1$ ,  $a^{-1} \notin \mathbb{Z}$ .

(e) Associativity:

$$\begin{aligned}(a * b) * c &= (ab) * c \\ &= (ab) c \\ &= a(bc) \\ &= a * (bc)\end{aligned}$$

Inverses: Select  $a \in \mathbb{R}$ ,

$$a * a = a \frac{1}{a} = 1$$

Closure: Obvious from closure of  $(\mathbb{R}, \cdot)$

Identity: 1 is the identity, Obvious from  $(\mathbb{R}, \cdot)$

(f) Associativity:

$$\begin{aligned}(a * b) * c &= (ab) * c \\ &= (ab) c \\ &= a(bc) \\ &= a * (bc)\end{aligned}$$

Inverses: Select  $a \in \mathbb{Q}$ ,

$$a * a^{-1} = a \frac{1}{a} = 1$$

Closure:  $a, b \in \mathbb{Q}$ ,  $a = \frac{p_1}{q_1}$   $b = \frac{p_2}{q_2}$ ,  $p_1, q_1, p_2, q_2 \in \mathbb{Z}$ ,  $q_1 \neq 0 \neq q_2$ .

$$\begin{aligned}a * b &= ab \\ &= \frac{p_1 p_2}{q_1 q_2} \in \mathbb{Q}\end{aligned}$$

Identity: 1 is the identity, Obvious from  $(\mathbb{R}, \cdot)$

3. Let  $(G, \cdot)$  be a group. Define a new binary operation  $*$  on  $G$  by the formula  $a * b = b \cdot a$ , for all  $a, b \in G$ .

(a) Show that  $(G, \cdot)$  is a group.

(b) Give examples to show that  $(G, \cdot)$  may or may not be the same as  $(G, *)$ .

### Joe Starr

(a) Associativity:

$$\begin{aligned} (a * b) * c &= (b \cdot a) * c \\ &= c \cdot (b \cdot a) \\ &= (c \cdot b) \cdot a \\ &= (b * c) \cdot a \\ &= a * (b * c) \end{aligned}$$

Inverses: Let  $a \in G$  since  $(G, \cdot)$  is a group we know  $a^{-1} \in G$ . Now  $a * a^{-1} = a^{-1} \cdot a = 1$ .

Closure: We select  $a, b \in G$  consier  $a * b = b \cdot a$  by closure of  $(G, \cdot)$ ,  $a * b \in G$ .

Identity: Let  $a \in G$ , consider  $1 * a = a \cdot 1 = a$  and  $a * 1 = 1 \cdot a = a$ .

(b) Let  $G =$ 

$\cdot$	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

 so  $a * b = b \cdot a = f$  but  $a \cdot b = d$ . In this case they are not equal.

If we let  $G = (\mathbb{Z}, +)$ , we have  $a * b = b + a = a + b$ . In this case they are equal.

5. Is  $GL_n(\mathbb{R})$  an Abelian group? Support your answer by either proof or a counter example.

**Joe Starr**

No, select

$$A = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} B = \begin{bmatrix} 11 & 13 \\ 17 & 19 \end{bmatrix}$$

we calculate

$$AB = \begin{bmatrix} 73 & 83 \\ 174 & 198 \end{bmatrix} BA = \begin{bmatrix} 87 & 124 \\ 129 & 184 \end{bmatrix}$$

8. Write out the multiplication table for the following set of matrices over  $\mathbb{Q}$ :

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

**Joe Starr**

Let

$$i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, j = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, k = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, l = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$\cdot$	$i$	$j$	$k$	$l$
$i$	$i$	$j$	$k$	$l$
$j$	$j$	$i$	$l$	$k$
$k$	$k$	$l$	$i$	$j$
$l$	$l$	$k$	$j$	$i$

9. Let  $G = \{x \in \mathbb{R} | x > 0 \text{ and } x \neq 1\}$ . Define the operation  $*$  on  $G$  by  $a * b = a^{\ln b}$ , for all  $a, b \in G$ . Prove that  $G$  is an Abelian group under the operation  $*$ .

**Joe Starr**

Associativity:

$$\begin{aligned}(a * b) * c &= (a^{\ln b}) * c \\ &= (a^{\ln b})^{\ln c} \\ &= a^{\ln b \ln c} \\ &= a^{\ln b^{\ln c}} \\ &= a * (b * c)\end{aligned}$$

Inverses: Let  $a \in G$ , consider  $a^{-1} = e^{\frac{1}{\ln a}}$ .

$$\begin{aligned}a * a^{-1} &= a^{\ln a^{-1}} \\ &= a^{\ln e^{\frac{1}{\ln a}}} \\ &= a^{\frac{1}{\ln a}} \\ &= a^{\log_a e} \\ &= e\end{aligned}$$

$$\begin{aligned}a^{-1} * a &= (a^{-1})^{\ln a} \\ &= (e^{\frac{1}{\ln a}})^{\ln a} \\ &= (e^{\log_a e})^{\ln a} \\ &= (e^{\ln a})^{\log_a e} \\ &= a^{\log_a e} \\ &= e\end{aligned}$$

Closure: Let  $a, b \in G$ ,  $a * b = a^{\ln b}$  we know that  $b > 0$  so  $\ln b$  exists, further since  $1 \notin G$  we have  $\ln b \neq 0$ . We observe that for any  $a \in G$   $a^{\ln b} > 0$  since  $a > 0$  and since  $\ln b \neq 0$   $a^{\ln b} \neq 1$ .

Identity: Our conjecture is that  $e$  is the identity element. Let  $a \in G$ ,  $e * a = e^{\ln a} = a$  and  $a * e = a^{\ln e} = a$

10. Show that the set  $A = \{f_{m,b} : \mathbb{R} \rightarrow \mathbb{R} | m \neq 0 \text{ and } f_{m,b} = mx + b\}$ . of affine functions from  $\mathbb{R}$  to  $\mathbb{R}$  forms a group under function composition.

**Joe Starr**

Associativity: We've proved this previously.

Inverses: Let  $f \in A$ ,  $f(x) = mx + b$ . Consider  $I(x) = \frac{1}{m}(x - b)$

$$\begin{array}{l|l} f(I(x)) = m\left(\frac{1}{m}(x - b)\right) + b & I(f(x)) = \frac{1}{m}((mx + b) - b) \\ = x - b + b & = \frac{1}{m}(mx) \\ = x & = x \end{array}$$

Closure: Let  $f, g \in A$ , so  $f(x) = m_1x + b_1$  and  $g(x) = m_2x + b_2$ . Now composing  $f$  and  $g$   $f(g(x))$ .

$$\begin{aligned} f(g(x)) &= m_1(m_2x + b_2) + b_1 \\ &= m_1m_2x + m_1b_2 + b_1 \\ &= mx + m_1b_2 + b_1 \\ &= mx + b \end{aligned}$$

Identity: Let  $f \in A$ ,  $f(x) = mx + b$ . Conjecture  $e(x) = x$

$$\begin{array}{l|l} f(e(x)) = m(x) + b & e(f(x)) = mx + b \\ = mx + b & \end{array}$$

11. Show that the set of all  $2 \times 2$  matrices over  $\mathbb{R}$  of the form  $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$  with  $m \neq 0$  forms a group under matrix multiplication.

**Joe Starr**

Let  $G$  be the set of all  $2 \times 2$  matrices over  $\mathbb{R}$  of the form  $\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$  with  $m \neq 0$ .

Associativity: Free from  $M_2(\mathbb{R})$

Inverses: Let  $a \in G$ , so  $a = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$  we can calculate the determinate of  $a$ .  $m \cdot 1 - b \cdot 0 = m$  and by definition of the set  $m \neq 0$ . So we have inverses.

Closure: Let  $a, b \in G$ , so  $a = \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix}$  and  $b = \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix}$

$$\begin{aligned} ab &= \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} m_2 m_1 & b_1 + m_1 b_2 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Identity: Free from  $M_2(\mathbb{R})$



























## 3.2 Subgroups

2.

Joe Starr























































## 4 Section

I <3 my Wayne State Libraries! Do you?

### 4.1 A Subsection

## 5 Section

I <3 my Wayne State Libraries! Do you?

### 5.1 A Subsection

## 6 Section

I <3 my Wayne State Libraries! Do you?

### 6.1 A Subsection

## 7 Section

I <3 my Wayne State Libraries! Do you?

### 7.1 A Subsection

## 8 Section

I <3 my Wayne State Libraries! Do you?

### 8.1 A Subsection



## 9 Section

I <3 my Wayne State Libraries! Do you?

### 9.1 A Subsection

## 10 Section

I <3 my Wayne State Libraries! Do you?

### 10.1 A Subsection