WAYNE STATE
UNIVERSITY

Algebra I
Winter 2020

Contents

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 $n = s$.

3. Find the quotient and reminder when a id divided by b.

a $a = 99$, $b = 17$

b $a = -99$, $b = 17$

c $a = 17$, $b = 99$

d $a = -1017$, $b = 99$

Joe Starr

a $99 = 17q + r \Rightarrow q = 5, r = 14$

b $-99 = 17q + r \Rightarrow q = -6, r = 3$

c $17 = 99q + r \Rightarrow q = 0, r = 17$

d $-1017 = 99q + r \Rightarrow q = -11, r = 72$

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) $(6643, 2873)$

$$\begin{aligned} 6643 &= 2873 * 2 + 897 \\ 2873 &= 897 * 3 + 182 \\ 897 &= 182 * 4 + 169 \\ 182 &= 169 * 1 + 13 \\ 169 &= 13 * 13 \end{aligned}$$

(b) $(7684, 4148)$

$$\begin{aligned} 7684 &= 4148 * 1 + 3536 \\ 4148 &= 3536 * 1 + 612 \\ 3536 &= 612 * 5 + 476 \\ 612 &= 476 * 1 + 136 \\ 476 &= 136 * 3 + 68 \\ 136 &= 68 * 68 \end{aligned}$$

(c) $(26460, 12600)$

$$\begin{aligned} 26460 &= 12600 * 2 + 1260 \\ 12600 &= 1260 * 10 \end{aligned}$$

(d) $(6540, 1206)$

$$\begin{aligned} 6540 &= 1206 * 5 + 510 \\ 1206 &= 510 * 2 + 186 \\ 510 &= 186 * 2 + 138 \\ 186 &= 138 * 1 + 48 \\ 138 &= 48 * 2 + 42 \\ 48 &= 42 * 1 + 6 \\ 42 &= 6 * 7 \end{aligned}$$

(e) $(12091, 8439)$

$$\begin{aligned} 12091 &= 8439 * 1 + 3652 \\ 8439 &= 3652 * 2 + 1135 \\ 3652 &= 1135 * 3 + 247 \\ 1135 &= 247 * 4 + 147 \\ 247 &= 147 * 1 + 100 \\ 147 &= 100 * 1 + 47 \\ 100 &= 47 * 2 + 6 \\ 47 &= 6 * 7 + 5 \\ 6 &= 5 * 1 + 1 \\ 5 &= 1 * 5 \end{aligned}$$

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, $nq_1 + nq_2 = n\left(q_1 + q_2\right) = nq$ 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,

$$\begin{aligned} 10n + 3 &= (5n+2)\,1 + (5n+1) \\ 5n + 2 &= (5n+1)\,1 + 1 \end{aligned}$$

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,

$$(2k) + 2 = (2k)\,1 + (2)$$
$$2k = (2)\,k$$

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,

$$\begin{aligned} a &= 2r + 1 \\ b &= 2s + 1 \end{aligned}$$

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

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

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

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

as desired.

1.2 Primes

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

(a) $(35, 14)$

(b) $(15, 11)$

(c) $(252, 11)$

(d) $(7684, 4148)$

(e) $(6643, 2873)$

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. US 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 $(n11)|n^2 - 1$, 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

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

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

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

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 $p|b$. WOLG 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 $d|(a + b) + (a - b) \to d|2a$ and $d|(a + b) - (a - b) \to d|2b$. 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 $b|m$,

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

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 definiton 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 $nn = \left(p_1^{n_1} \cdots p_k^{n_k}\right)\left(p_1^{n_1} \cdots p_k^{n_k}\right)$, by combining terms we can see that $nn = \left(p_1^{2n_1} \cdots p_k^{2n_k}\right)$, 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,

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

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,

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

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 $x = \log_3 2 \to 3^x = 2$, if x is rational then there exist m and n such that $\frac{m}{n} = x$. We now have $3^{\frac{m}{n}} = 2 \to 3^m = 2^n$, 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) $f : \mathbb{R} \to \mathbb{R}; f(x) = x + 3$

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

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

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

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

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

showing f a bijection.

(d) $f : \mathbb{R}^+ \to \mathbb{R}; f(x) = \ln x$ If we take $f^{-1}(x) = e^x$, $f(f^{-1}(x)) = \ln e^x = x$, showing f a bijection.

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

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

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

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

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

Joe Starr

(a) see question 1

(b) not a bijection

(c see question 1

(d) see question 1

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

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

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

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

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

Joe Starr

(a) Not a bijection

(b) Not a bijection

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

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

13. Let $f : A \to B$ be a function, and let $f(A) = \{f(a) | a \in A\}$ 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 $f : A \to B$ and $g : B \to C$ 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 tha $a \neq x$ 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 $a \neq b$, $g(f(x)) = g(f(a))$, 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 $f : A \to B$ 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 $h : B \to C$ and $k : B \to C$.

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 $f : A \to B$ 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 $h : C \to A$ and $k : C \to A$.

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:

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

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) $\sigma\tau$

(b) $\tau\sigma$

(c) $\tau^2\sigma$

(d) σ^{-1}

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

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

Joe Starr

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

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

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

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

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

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

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 σ and τ 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) $\tau^{-1}\sigma\tau = (1356)$

(σ) $\sigma = (13)\,(35)\,(56)$

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

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 it's 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:

$$\begin{tikzcd} & 1 \arrow[dl] & \\ 3 \arrow[rr] & & 10 \arrow[ul] \end{tikzcd} \qquad \begin{tikzcd} 2 \arrow[r] & 4 \arrow[d] \\ 7 \arrow[u] & 5 \arrow[l] \end{tikzcd} \qquad \begin{tikzcd} 6 \arrow[r, dash] & {} \arrow[d] \\ {} \arrow[u] & 8 \arrow[l, dash] \end{tikzcd}$$

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:
$(1, 3, 10) = 3$, $(2, 4, 5, 7) = 4$ $(6, 8) = 2$ order is 12

4. Find the oder of each of the following permutations.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 2 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 5 & 1 & 8 & 2 & 3 \end{pmatrix}$

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

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

Joe Starr

(a) $(1,6)\,(2,4,2,5)$ order is 4

(b) $(1,4,5)\,(2,6,8,3,7)$ order 15

(c) $(1,5,3,8)\,(2,9)\,(4,7,6)$ order 12

(d) $(1,8)\,(2,4,6)\,(3,9,7)$ order 6

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

Joe Starr

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

We can now compose τ^{-1} and σ yielding $(m, m-1, 1, 2, \ldots, m-3, m-2)$.

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:

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

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:

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

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 $a * b = b \cot a$, 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 $\mathrm{GL}_n(\mathbb{R})$ 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

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

·	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 $G = \{x \in \mathbb{R} | x > 0 ext and x \neq 1\}$. 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:

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

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

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

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

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 $A = \{f_{m,b} : \mathbb{R}o\mathbb{R} | m \neq 0 ext and f_{m,b} = mx + b\}$. 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 $I(x) = \frac{1}{m}(x - b)$

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

$$\begin{aligned} I(f(x)) &= \frac{1}{m}((mx+b) - b) \\ &= \frac{1}{m}(mx) \\ &= x \end{aligned}$$

Closure: Let $f, g \in A$, so $f(x) = m_1 x + b_1$ and $g(x) = m_2 x + b_2$. Now composing f and g $f(g(x))$.

$$\begin{aligned} f(g(x)) &= m_1(m_2 x + b_2) + b_1 \\ &= m_1 m_2 x + m_1 b_2 + b_1 \\ &= mx + m_1 b_2 + b_1 \\ &= mx + b \end{aligned}$$

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

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

$$e(f(x)) = mx + b$$

11. Show that the set of all $2imes2$ 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 $2imes2$ 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. $m1 - b0 = m$ 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 $M_2(\mathbb{R})$

12. In the group defined in question 11 find all elements that commute with $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$

Joe Starr

We can begin by letting $a \in G$ calculating $a \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} a$.

$$\begin{aligned} a \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2m & b \\ 0 & 1 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} a &= \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 2m & 2b \\ 0 & 1 \end{bmatrix} \end{aligned}$$

So for a matrix of to commute with $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ it must be of the form $\begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix}$.

13. Define $*$ on $\mathbb{R}$ by $a * b = a + b - 1$, for all $a, b \in \mathbb{R}$. Show that $(\mathbb{R}, *)$ is an Abelian group.

Joe Starr

Abelian:

$$\begin{aligned} a * b &= a + b - 1 \\ &= b + a - 1 \\ &= b * a \end{aligned}$$

Associativity:

$$\begin{aligned} (a * b) * c &= (a + b - 1) * c \\ &= (a + b - 1) + c - 1 \\ &= a + b + c - 1 - 1 \\ &= a + (b + c - 1) - 1 \\ &= a * (b * c) \end{aligned}$$

Inverses: Let $a \in (\mathbb{R}, *)$, consider $a^{-1} = 2 - a$

$$\begin{aligned} a * a^{-1} &= a + (2 - a) - 1 \\ &= 1 \end{aligned}$$

$$\begin{aligned} a^{-1} * a &= (2 - a) + a - 1 \\ &= 1 \end{aligned}$$

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

Identity: Conjecture is that 1 is the identity element of $(\mathbb{R}, *)$.

$$\begin{aligned} a * 1 &= a + 1 - 1 \\ &= a \end{aligned}$$

$$\begin{aligned} 1 * a &= a + 1 - 1 \\ &= a \end{aligned}$$

Joe Starr

Let $\varphi : (\mathbb{R}, *) \, o \, (\mathbb{R}, +)$, with $\varphi(x) = x - 1$, $\varphi(a * b) = (a + b - 1) - 1 = a - 1 + b - 1 = \varphi(a) + \varphi(b)$. Further $\varphi^{-1}(x) = x + 1$, $\varphi\left(\varphi^{-1}(x)\right) = (x + 1) - 1 = x$. Showing a group structure isomorphic to $(\mathbb{R}, +)$.

14. Let $S = \mathbb{R} - \{\text{-}1\}$. Define $*$ on S by $a * b = a + b + ab$ for all $a, b \in S$. Show that $(S\,,\,*)$ is an Abelian group.

Joe Starr

Abelian:

$$\begin{aligned} a * b &= a + b + ab \\ &= b + a + ba \\ &= b * a \end{aligned}$$

Inverses: Consider $a^{\text{-}1} = \frac{\text{-}a}{a+1}$

$$\begin{aligned} a * a^{\text{-}1} &= a + \frac{\text{-}a}{a+1} + a\frac{\text{-}a}{a+1} \\ &= a + \frac{\text{-}a\,(a+1)}{a+1} \\ &= a + \text{-}a \\ &= 0 \end{aligned}$$

Closure: Let $a, b \in \mathbb{R}$, if we take $a * b = a + b + ab$. Assume that $a * b = \text{-}1$

$$\begin{aligned} \text{-}1 = a + b + ab &\Rightarrow \text{-}1 - a = b + ab \\ &\Rightarrow \text{-}1 - a = b\,(1 + a) \\ &\Rightarrow \text{-}\frac{a+1}{1+a} = b \\ &\Rightarrow \text{-}1 = b \end{aligned}$$

a contradiction.

Identity: Conjecture is that 0 is the identity element of $(S\,,\,*)$.

$$\begin{aligned} a * 0 &= a + 0 + a0 \\ &= a \end{aligned}$$

Associativity:

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= a + b + ab + c + ca + cb + cab \\ &= a + (b + c + bc) + a\,(b + c + bc) \\ &= a * (b + c + bc) \\ &= a * (b * c) \end{aligned}$$

15. Let $G = \{x \in \mathbb{R} | x > 1\}$. Define $*$ on G by $a * b = ab - a - b + 2$, for all $a, b \in G$. Show that $(G\,,\,*)$ is an Abelian group.

Joe Starr

Abelian:

$$\begin{aligned} a * b &= ab - a - b + 2 \\ &= ba - b - a + 2 \\ &= b * a \end{aligned}$$

Inverses: Consider $a^{\text{-}1} = \frac{a}{a-1}$

$$\begin{aligned} a * a^{\text{-}1} &= a\frac{a}{a-1} - a - \frac{a}{a-1} + 2 \\ &= \frac{a}{a-1}\left(a-1\right) - a + 2 \\ &= a - a + 2 \\ &= 2 \end{aligned}$$

Identity: Conjecture is that 2 is the identity element of $(G\,,\,*)$.

$$\begin{aligned} a * 2 &= a2 - a - 2 + 2 \\ &= a \end{aligned}$$

Closure: We begin by letting $a, b \in G$, we observe $a \geq b > 1$. We can then multiply through by b yeilding $ab \geq bb > b > 1$. Next we subtract both a and b, $ab - a - b \geq 1 > \text{-}a$, finaly adding two gives $ab - a - b + 2 \geq 3$ showing $a * b \in G$.

Associativity:

$$\begin{aligned} (a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= (a + b + ab) + c + (a + b + ab)\,c \\ &= a + b + ab + c + ca + cb + cab \\ &= a + (b + c + bc) + a\,(b + c + bc) \\ &= a * (b + c + bc) \\ &= a * (b * c) \end{aligned}$$

16. Let G be a group. We have shown that $(ab)^{-1} = b^{-1}a^{-1}$. Find a similar expression for $\left(abc^{-1}\right)$

Joe Starr

We will use a transitive proof:

$$\begin{aligned}(abc)^{-1} &= c^{-1}\,(ab)^{-1} \\ &= c^{-1}b^{-1}a^{-1}\end{aligned}$$

17. Let G be a group. If $g \in G$ and $g^2 = g$,then prove that $g = e$.

Joe Starr

We begin with letting $g \in G$, such $g^2 = g$ we then multiply by g^{-1} on the left:

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

as desired.

18. Show that a nonabelian group must have at least 5 elements.

Joe Starr

Let G be a nonabelian group. Since G a group then $e \in G$ the identity. G can't be the trivial group since the trivial group is Abelian, this puts $a \in G$ with $a \neq e$ further $a^{-1} \in G$. With the same argument G is not a group of three elements, so $b, b^{-1} \in G$. This puts $a, b, b^{-1}, a^{-1}, e \in G$ showing G with at lest 5 elements.

22. Let S be a nonempty finite set with a binary operation $*$ that satisfies the associative law. Show that S is a group if $a * b = a * c$ implies $b = c$ and $a * c = b * c$ implies $a = b$ for all $a, b, c \in S$. What can we say if S is infinite?

Joe Starr

24. Let G be a group. Prove that G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

Joe Starr

wocase Let G be an abelian group and $a, b \in G$. Consider $(ab)^{-1}$, we have shown $(ab)^{-1} = b^{-1}a^{-1}$ since G is abelian we have $(ab)^{-1} = a^{-1}b^{-1}$. Let $(ab)^{-1} = a^{-1}b^{-1}$, we have shown $(ab)^{-1} = b^{-1}a^{-1}$ so $b^{-1}a^{-1} = a^{-1}b^{-1}$ showing G abelian.

25. Let G be a group. Prove that if $x^2 = e$ for all $x \in G$, then G is abelian.

Joe Starr

Let G be a group with the given property $a, b \in G$. Observe that $a^2 = e \Rightarrow a = a^{-1}$. We have shown that $(ab)^{-1} = b^{-1}a^{-1}$. We proceed with a transitive proof:

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

showing G abelian as desired.

26. Show that if G is a finite group with an even number of elements, then there must exist an element $a \in G$ with $a \neq e$ such that $a^2 = e$.

Joe Starr

Let G be a group with the given property. Since G a group $e \in G$. Observe G is not the trivial group since it has even cardinality. If we consider the cardinality of G/e it's $|G| - 1$ an odd number. Let $a \in G$ with $a \neq e$, observe that since G a group $a^{-1} \in G$. We are left with two possibilities $a = a^{-1}$ or $a \neq a^{-1}$. If $a = a^{-1}$ we are done, otherwise we can delete a and a^{-1} from G and select from the remaining elements of G. Since G/e has odd cardinality we can repeat this process until there is a single element remaining. It must be that $a = a^{-1}$ as desired.

3.2 Subgroups

1. In $\mathrm{GL}_2(\mathbf{R})$, find the order of each of the following elements.

(a)† $\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ †(c) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (d) $\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$

Joe Starr

(a)

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^6 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(b)

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(c)

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

Infinite order.

(d)

$$\begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2. Let $A = \begin{bmatrix} 1 & \text{-}1 \\ \text{-}1 & 0 \end{bmatrix} \in \mathrm{GL}_2(\mathrm{R})$. Show that A has infinite order by proving that $A^n = \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix}$, for $n \geq 1$, where $F_0 = 0, F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ is the Fibonacci sequence.

Joe Starr

We will proceed with induction:

Base Case: Consider 1 for the basecase. $\begin{bmatrix} F_{n+1} & \text{-}F_n \\ \text{-}F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & \text{-}1 \\ \text{-}1 & 0 \end{bmatrix}$ showing the base case to be true.

Inductive Case: Assume that it's ture for the nth power we will show this implies the $n+1$th case to be true.

$$A^{n+1} = A^n A^1 = \begin{bmatrix} F_{n+1} & \text{-}F_n \\ \text{-}F_n & F_{n-1} \end{bmatrix} \begin{bmatrix} 1 & \text{-}1 \\ \text{-}1 & 0 \end{bmatrix} = \begin{bmatrix} F_{n+2} & \text{-}F_{n+1} \\ \text{-}F_{n+1} & F_n \end{bmatrix}$$

showing the Inductive case to be true, and A of infinite order.

3. Prove that the set of all rational numbers of the form m/n, where $m, n \in \mathbf{Z}$ and n is square-free, is a subgroup of Q (under addition).

Joe Starr

Inverses: Let $m, n \in \mathbb{Z}$ with the given properties. Take $\frac{-m}{n}$ and consider $\frac{m}{n} + \frac{-m}{n} = \frac{m-m}{n} = 0$ as desired.

Closure: Let $m, n, a, b \in \mathbb{Z}$ with the given properties. Take $\frac{m}{n} + \frac{a}{b} = \frac{mb+an}{bn}$, since b and n are square free bn is also square free.

4. Show that $\{\ (1),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\ \}$ is a subgroup of S_4

Joe Starr

Inverses:

Closure:

6. Let $G = \mathrm{GL}_2(\mathbf{R})$ (a) Show that $T = \left\{ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} | ad \neq 0 \right\}$ is a subgroup of G. (b) Show that $D = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} | ad \neq 0 \right\}$ is a subgroup of G.

Joe Starr

7. Let $G = \mathrm{GL}_2(\mathrm{R})$. Show that the subset S of G defined by $S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} | b = c \right\}$ of symmetric $2imes2$ matrices does not form a subgroup of G.

Joe Starr

8. Let $G = \mathrm{GL}_2(\mathrm{R})$. For each of the following subsets of $M_2(\mathbf{R})$, determine whether or not the subset is a subgroup of G. (a) $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} | ab \neq 0 \right\}$ (b) $B = \left\{ \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} | bc \neq 0 \right\}$ (c) $C = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} | c \neq 0 \right\}$

Joe Starr

9. # Let $G = \mathrm{GL}_3(\mathbf{R})$. Show that $H = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{bmatrix} \right\}$ is a subgroup of G.

Joe Starr

10. Let m and n be nonzero integers, with $(\, m, n\,) = d$. Show that m and n belong to $d\mathbf{Z}$, and that if H is any subgroup of $\mathbf{Z}$ that contains both m and n, then $d\mathbf{Z} \subseteq H$

11. Let S be a set, and let a be a fixed element of S. Show that $\{\sigma \in \mathrm{Sym}(S) | \sigma(a) = a\}$ is a subgroup of $\mathrm{Sym}(S)$

Joe Starr

12. + For each of the following groups, find all elements of finite order. (a) $\mathbf{R}^{imes}$ (b) $\mathbf{C}^{imes}$

Joe Starr

13. Let G be an abelian group, such that the operation on G is denoted additively. Show that $\{a \in G | 2a = 0\}$ is a subgroup of G. Compute this subgroup for $G = \mathbf{Z}_{12}$

Joe Starr

14. Let G be an abelian group, and let H be the set of all elements of G of finite order. (a) Show that H is a subgroup of G. (b) For a fixed positive integer k, show that $\{a \in G | exto(aext)isadivisorofk\}$ is a subgroup of H (c) For a fixed positive integer k, is $\{a \in G | o(a) \leq k\}$ a subgroup of H? Either give a proof or give a counterexample.

Joe Starr

15. Prove that any cyclic group is abelian.

Joe Starr

16. Prove or disprove this statement. If G is a group in which every proper subgroup is cyclic, then G is cyclic.

Joe Starr

17. # Prove that the intersection of any collection of subgroups of a group is again a subgroup.

Joe Starr

18. Let G be the group of rational numbers, under addition, and let H, K be subgroups of G. Prove that if $H \neq \{0\}$ and $K \neq \{0\}$, then $H \cap K \neq \{0\}$.

Joe Starr

19. Let G be a group, and let $a \in G$. The set $C(a) = \{x \in G | xa = ax\}$ of all elements of G that commute with a is called the centralizer of a. $\#(exta) Show that C(a) extisasubgroupof G$ (b) Show that $\langle a \rangle \subseteq C(a)$ (c) Compute $C(a)$ if $G = S_3$ and $a = (1, 2, 3)$ (d) Compute $C(a)$ if $G = S_3$ and $a = (1, 2)$

Joe Starr

20. Compute the centralizer in $\mathrm{GL}_2(\mathbf{R})$ of the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Joe Starr

22. Show that if a group G has a unique element a of order 2, then $a \in Z(G)$

Joe Starr

23. If the group G is not abelian, show that its center $Z(G)$ is a proper subgroup of an abelian subgroup of G.

Joe Starr

26. Let G be a group with $a, b \in G$. (a) Show that $o\left(a^{-1}\right) = o(a)$ (b) Show that $o(ab) = o(ba)$ (c) Show that $o\left(aba^{-1}\right) = o(b)$

Joe Starr

27. Let G be a finite group, let $n > 2$ be an integer, and let S be the set of elements of G that have order n. Show that S has an even number of elements.

Joe Starr

28. Let G be a group with $a, b \in G$. Assume that $o(a)$ and $o(b)$ are finite and relatively prime, and that $ab = ba$. Show that $o(ab) = o(a)o(b)$

Joe Starr

29. Find an example of a group G and elements $a, b \in G$ such that a and b each have finite order but ab does not.

Joe Starr

2.

Joe Starr

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

11 General Proofs

11.1 $a + b < ab$ for $a > 2$ and $b > 2$

Joe Starr

$a > b$: Here we assume $ab < a + b$ divide by b $a < \frac{a}{b} + 1$ since $a > b$ $\frac{a}{b} > 1$ so $\frac{a}{b} + 1 > 2$ so $b < 2$ a contradiction.

$a = b$: Here we assume $a^2 < 2a$ divide by a $a < 2$ a contradiction.

11.2 $a + b > ab$ for $2 > a > 1$ and $2 > b > 1$

Joe Starr

$a > b$: Here we assume $ab > a + b$ divide by b $a > \frac{a}{b} + 1$ since $a > b$ $\frac{a}{b} > 1$ so $\frac{a}{b} + 1 > 2$ so $a > 2$ a contradiction.

$a = b$: Here we assume $a^2 > 2a$ divide by a $a > 2$ a contradiction.

11.3 $a + b > ab$ for $a > 2 > b > 1$

Joe Starr

Here we assume $ab > a + b$ divide by a $b > \frac{b}{a} + 1$ since $a > b$, $\frac{b}{a} < 1$ so $\frac{a}{b} + 1 < 2$ so $a > 2$ a contradiction.